CEMP-ET Engineer Pamphlet 1110-3-7	Department of the Army U.S. Army Corps of Engineers Washington, DC 20314-1000	EP 1110-3-7 15 December 1994
	Engineering and Design LOCAL AREA NETWORKS IN MILITARY CONSTRUCTION PROJECTS	
	Distribution Restriction Statement Approved for public release; distribution is unlimited.	

US ARMY CORPS
of ENGINEERS

EP 1110-3-7
December 1994

ENGINEERING AND DESIGN

LOCAL AREA NETWORKS
(LAN)

DEPARTMENT OF THE ARMY
U.S. Army Corps of Engineers
Washington, D.C. 20314-1000

CEMP-ET

DEPARTMENT OF THE ARMY
U.S. Army Corps of Engineers
Washington, D.C. 20314-1000

EP 1110-3-7

Pamphlet
No. 1110-3-7

15 December 1994

Engineering and Design
LOCAL AREA NETWORKS IN
MILITARY CONSTRUCTION PROJECTS

1. Purpose. This pamphlet transmits information which may be used for the design and implementation of local area networks (LAN) associated with military construction projects.

2. Applicability. This pamphlet applies to all HQUSACE/OCE elements, major subordinate commands, districts, and separate field operating activities (FAO) having military design and construction responsibility.

3. References. See Appendix A.

4. Background. This LAN design was developed by the U. S. Army Information Systems Command to provide guidance to the Director of Information Management. It has been adapted by the Corps of Engineers to provide design and implementation guidance for incorporating LANs into military construction projects. This guide provides a tutorial on a variety of different LAN architectures, a process for designing LANs, and a section on staffing, training, installation and network management. Site survey checklists are provided to assist the designer and provide a method to assure that user requirements are included in the final design.

FOR THE COMMANDER:

R. L. Vanantwerp

R. L. VANANTWERP
Colonel, Corps of Engineers
Chief of Staff

DESIGN GUIDE
FOR
LOCAL AREA NETWORKS (LAN)

TABLE OF CONTENTS

TABLE OF CONTENTS

Description Page

TABLE OF CONTENTS

Description Page

TABLE OF CONTENTS

TABLE OF CONTENTS

Description Page

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF CONTENTS

LIST OF FIGURES

TABLE OF CONTENTS

LIST OF FIGURES (Cont'd)

TABLE OF CONTENTS

LIST OF FIGURES (Cont'd)

EXAMPLE FIGURES

TABLE OF CONTENTS

EXAMPLE FIGURES (Cont'd)

LIST OF TABLES

SECTION 1. INTRODUCTION

PURPOSE

This local area network (LAN) design guide was developed as a guideline in determining what is required to implement a LAN. This document provides greater understanding of LAN operation in order to:

- develop a more comprehensive statement of work for a LAN design
- assist in developing and performing a site survey
- justify items in a site concurrence memorandum validate the Engineering Installation Plan (EIP) justify equipment and installation costs understand network components and operation examine acceptance test procedures for completeness
- confirm installation procedures provide guidelines for LAN operation and maintenance.

SCOPE

The major sections of this guide are outlined below.

LAN Tutorial

This section provides a standards-based overview of LAN operations, equipment, and software. It is used as a tutorial for those unfamiliar with LAN terminology and provides references for the design section.

LAN Design Process	This section provides instruction in the design of standards-based LANs that use 10BaseT, 10BaseF, and fiber distributed data interface (FDDI). Transmission media specified includes category 5 unshielded twisted pair (UTP) and multimode fiber optic cable. The design process presented in this guide covers a new LAN installation in new or existing buildings and covers BLACK or unclassified data only. This design process helps the user create a basic Ethernet LAN and three performance variations of that LAN. To assist the user in selecting a performance variation and estimate the cost of the LAN, a detailed cost model has been developed. The cost model presents the basic LAN design and the three performance variations in small, medium, and large configurations.
LAN Start-Up and Operations	This section provides guidelines for staffing and training, installation, and network management.
References	Appendix A contains a list of references used in this pamphlet.
Site Survey Checklists	Appendix B provides blank site survey checklists to be used in determining the needs of the proposed LAN.
Glossary	Terms and definitions used in this pamphlet are listed in the glossary.
Bibliography	Additional reading and source materials are listed in the bibliography.

SECTION 2. LAN TUTORIAL

This section defines LAN concepts, terminology, and components. All information is in compliance with International Standards Organization (ISO), International Electrotechnical Commission (IEC), Institute of Electrical and Electronics Engineers (IEEE), and American National Standards Institute (ANSI) standards.

WHAT IS A NETWORK

With the development of personal computers (PC) in the 1980s, more and more computer oriented operations were interconnecting terminals, desktop computers, printers, micro and minicomputers, mainframes, and other information processing equipment. Interconnection quickly grew in popularity because it enhanced the communication capabilities and lowered the cost of user/computer arrangements The organization of communications channels making this interconnection possible, shown in figure 2-1, was termed a computer network.

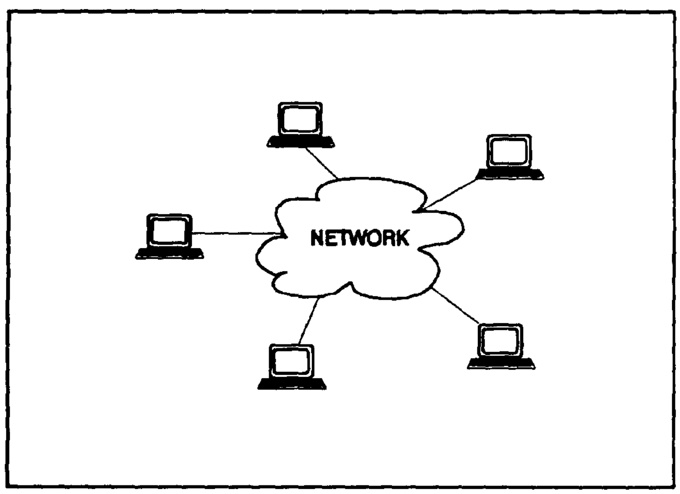


FIGURE 2-1. Interconnection; the network.

WHAT IS A LAN

A LAN is a computer network that operates within a limited geographic area, such as an office, a building, or a small cluster of buildings. It operates at speeds of 1 megabits per second (Mbps) to over 100 Mbps. LANs are generally privately owned networks, which are controlled by their owners.

WHAT IS A WAN

A wide area network (WAN) is a computer network that spans a large geographical area, for example, states, countries, and continents. Figure 2-2 shows that a WAN is used to interconnect distant computers or LANs, which are too far apart to interconnect using a single device.

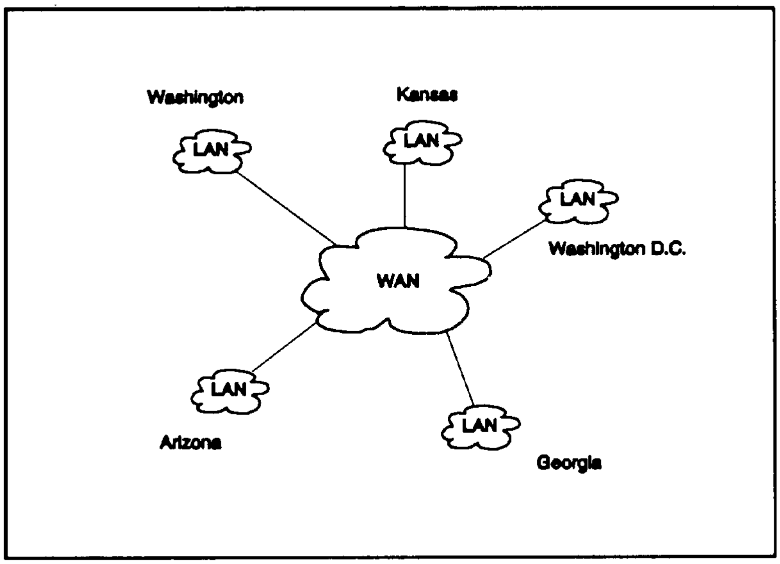


FIGURE 2-2. WAN.

WANs typically use a switching technology for data transmission and operate at speeds of 56 kilobits per second (kbps) or above. WANs use public communications services including digital data service (DDS) lines, T-1 or fractional T-1 circuits, T-3 circuits, and X.25 public data networks.

BENEFITS OF A LAN

LANs provide resource sharing, improve reliability, reduce costs, increase worker productivity, and enhance group computer management.

Resource sharing enables LAN users to share software resources such as files and applications and hardware resources such as printers and plotters. Use of a LAN means that fewer printers, plotters, and other shared equipment must be purchased. Software licenses do not have to be purchased for each LAN user; only a single network or group license has to be acquired.

Improved reliability is provided by multiple access to resources. Critical files and applications can reside on more than one computer. If one computer goes down, the LAN user can still access resources from another computer.

Cost savings are realized as a result of distributed processing. When a mainframe computer is the sole source of processing power, users who are not collocated require direct communication lines, and leased public service communications cost money. In addition, distributed processing on smaller computers provides a better price/performance ratio than processing on a central mainframe.

LANs increase worker productivity and therefore decrease personnel costs. They enable information sharing and decreased response times and eliminate or ease repetitive operations.

In terms of group computer management, LANs make centralized LAN user assistance groups a practical option for LAN user support. As a result of global network access, support groups are able to improve LAN user efficiency and decrease equipment down time.

OPEN SYSTEMS

Until the late 1980s, LAN vendors designed and produced hardware and software that functioned well on its own, but could not be used with the products of a different or third party vendor. LAN administrators who purchased a single vendor solution found themselves in a dilemma when it came to upgrading or purchasing additional hardware and software for their LANs. This was especially true if they could not achieve a desired level of operability using the equipment or architecture offered by the single vendor. An administrator had to decide whether to spend a considerable sum of money to upgrade the network to an open system, or go with a less acceptable solution and still be restricted by proprietary network architecture.

The OSI reference model

In 1983, the ISO proposed the Open Systems Interconnection (OSI) reference model. This model defines an international set of standard protocols for communication between different network architectures. These standard, vendor independent protocols promote worldwide connectivity and interoperability between application processes in networks. The model was designed and developed as a guideline so that hardware, application software, and network services would interoperate between vendors. Currently, OSI is supported by all major governments and principle computer/network manufacturers throughout the world.

The OSI layers

The OSI reference model organizes LAN connectivity into seven definable pieces or layers (a protocol stack). With respect to the purpose of each layer, ISO mandated protocols define how networking hardware and software is to handle data and transfer it across a network. Interoperability, the purpose for defining a standard protocol model, exists when there is compatibility between the protocol stack of one workstation or peripheral device and that of another. Each individual layer is able to communicate with the respective layer of a receiving station or intermediate translation device as long as the OSI reference model is supported. Figure 2-3 shows the protocol stacks of two stations attached to the same LAN and shows the data flow between the sending and receiving application processes.

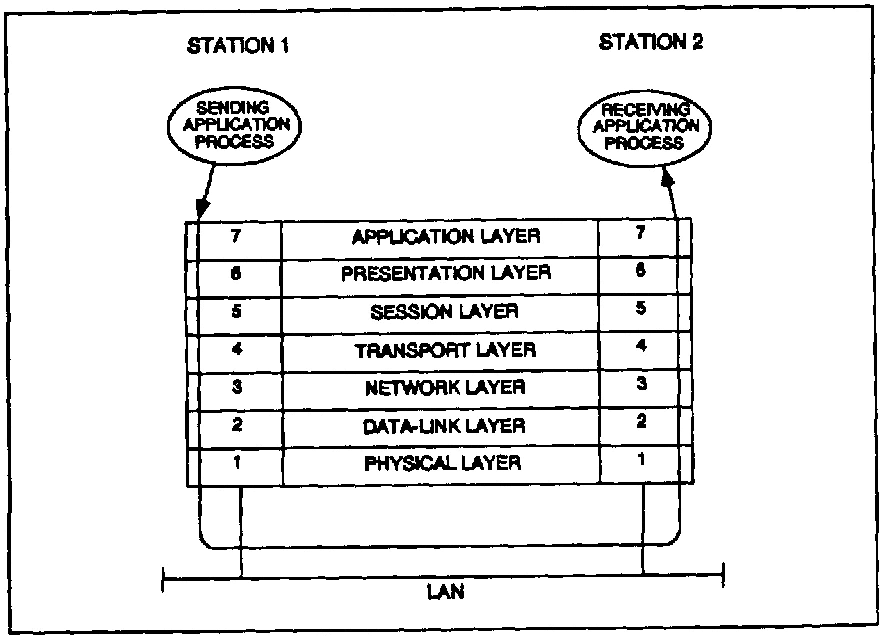


FIGURE 2-3. Data flow between protocol stacks.

Layer 7, *application layer*

The application layer (layer 7) allows for protocols and functions required by particular user-designed application processes. This layer contains functions that satisfy particular user requirements and application service elements that can be used by more than one application.

Layer 6, *presentation layer*

The presentation layer (layer 6) specifies or negotiates the way information is represented for exchange by application entities. The presentation layer provides the representation of: 1) data transferred between application entities, 2) the data structure that the application entities use, and 3) operations on the data's structure. The presentation layer uses a common syntax and semantics.

Layer 5, *session layer*

The session layer (layer 5) allows cooperating application entities to organize and synchronize conversation and manage data exchange. To transfer the data, session connections use transport connections. During a session, services are used by application entities to regulate dialogue by ensuring an orderly message exchange on the session connection. Examples include a LAN user logged onto a host across a network or a session established for the purpose of transferring files.

Layer 4, transport layer

The transport layer (layer 4) provides reliable, transparent transfer of data between cooperating session entities. The transport layer entities optimize the available network services to provide the performance required by each session entity. Optimization is constrained by the overall demands of concurrent session entities and by the quality and capacity of the network services available to the transport layer entities. The transport layer provides end-to-end data integrity by building on the error control mechanism provided by the lower layers.

Layer 3, network layer

The network layer (layer 3) provides message routing and relaying between end systems on the same network or on interconnected networks, independent of the transport protocol used. The network layer also provides hop-by-hop network service enhancements, flow control, uniform network address information scheme, and load leveling. Services provided by the network layer are independent of the distance separating interconnected networks. Interconnecting two dissimilar networks requires a uniform addressing scheme that can be understood by both networks. To have interoperability at layer 3, you must also have interoperability at the physical and data-link layers (layers 1 and 2).

Layer 2, data-link layer

The data-link layer (layer 2) provides communication between adjacent or broadcast Systems. The data-link layer performs frame formatting, error checking, addressing, and other functions necessary to ensure accurate data transmission between adjacent systems.

Layer 1, physical layer

The physical layer (layer 1) provides a physical connection for transmission of data between data-link entities. Physical entities perform electrical encoding and decoding of the data for transmission over a medium and regulate access to the physical network.

GOSIP

On 15 August 1990, the U.S. Government Open Systems Interconnection Profile (GOSIP), Version 1, became mandatory for federal systems procurement. GOSIP, a specification developed from a series of workshops conducted at the National Institute of Standards and Technology (NIST), identifies a subset of OSI protocols which are to be included in all government networks. As an implementation document for OSI, GOSIP is to be used by all federal government agencies acquiring network products and services.

GOSIP, Version 1, does not require that government agencies discontinue using computer networking products currently in use. GOSIP does direct all government agencies to requisition computer networking products that have OSI capabilities in addition to any other requirements.

GOSIP is a living document that is updated every year in order to track advancing LAN technologies. Figure 2-4 shows the current GOSIP protocol architecture.

A federal agency can verify whether a product is GOSIP-compliant by referring to a set of registers published by NIST. The most important register is Conformance Tested GOSIP Products which lists products successfully tested in an accredited test laboratory by an approved method of testing. The complete list of registers is:

- GOSIP Abstract Test Suites
- Assessed& Means of Testing
- National Voluntary Laboratory Accreditation Program Accredited Test Laboratories
- Conformance Tested GOSIP Products
- Interoperability Test Suites
- Interoperability Testing Services

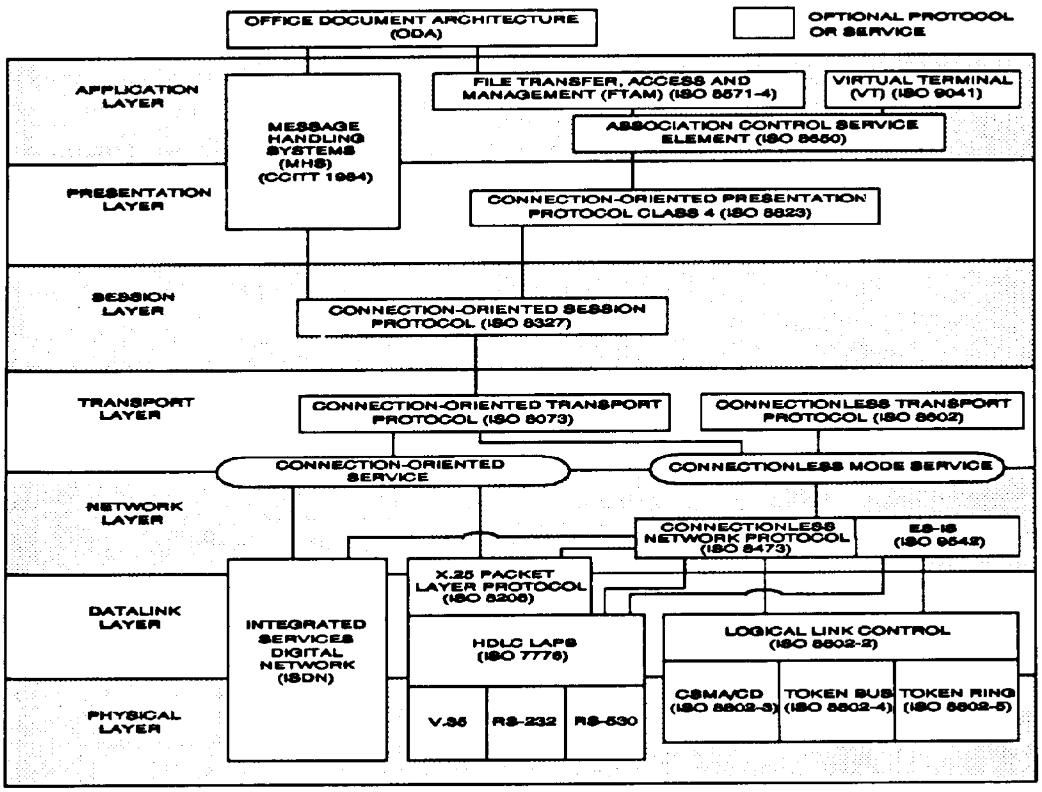


FIGURE 2-4. GOSIP OSI architecture.

- Interoperable GOSIP Products
- GOSIP Reference Implementations.

TCP/IP

Prior to open systems and the development of GOSIP, the military's primary interest in networking involved interconnecting dissimilar computer systems. Because of this interest, in the 1970s, the Defense Advanced Research Projects Agency (DARPA), an agency of the U.S. Department of Defense (DoD), began to develop a suite of protocols which would allow the necessary interconnections. The result of the research was Transmission Control Protocol/Internet Protocol (TCP/IP).

TCP is a transport protocol that fits into layer 4 of the OSI model. IP is a network protocol that fits into layer 3 of the OSI model. TCP provides end-to-end transmission control. IP provides uniform network addressing, routing of the transport protocol, and fragmentation and reassembly for long messages.

TCP/IP worked so well, that in 1983, the Office of the Secretary of Defense designated TCP/IP as a networking standard. Today, TCP/IP is the predominant method of internetworking and is common in the DoD networking environment.

LAN ARCHITECTURES

The key components of a LAN (infrastructure) architecture are topology, media access control (MAC), transmission media, and signaling method.

Topology

Topology is the map or plan of a network. For a single LAN, there is a physical topology and a logical topology. The physical topology is the pattern generated by the interconnection of cables and hardware devices in the network. The logical topology is the pattern of the flow of messages, independent of the physical layout.

The three basic topologies, whether physical or logical, are the bus, star, and ring.

Bus

The bus topology is a common shared cable terminated on both ends, as shown in figure 2-5.

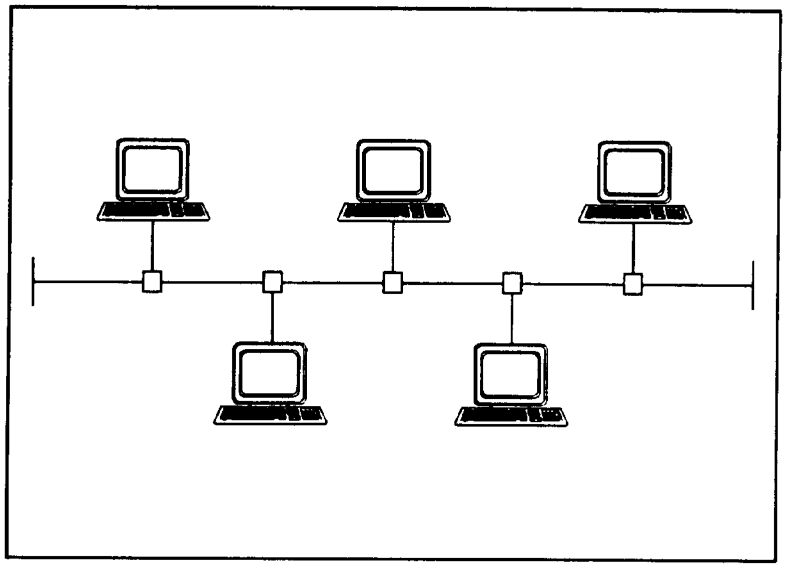


FIGURE 2-5. Bus topology.

Taps are used to attach stations along the cable length. The bus is frequently referred to as a broadcast medium, because transmissions are sent to all equipment attached to the LAN backbone, even if addressed to only one station. Each piece of equipment determines whether a message is addressed to it, and if so, accepts it, and if not, ignores it.

The bus is an easy topology to configure, expand on, and connect to. A broken connection between the bus backbone and a LAN user or an inactive station normally will not disrupt the rest of the network.

The disadvantage of the bus topology is that any failure of the transmission medium brings down the entire LAN. Also, locating the source of the problem can be difficult.

Examples of the implementation of bus topology are ISO/IEC 8802-3 Ethernet on thinnet (10Base2) or thicknet (10Base5), and the collapsed backbone inside a high-speed router. Additional information about the collapsed backbone may be found in this section in the hub portion of networking devices.

Star

The physical star topology is configured around a central wiring device or switching element, usually an intelligent hub, as shown in figure 2-6. The hub is a crossroad for electrical signals, using a high-speed backplane (bus) to which segments (users) are attached.

A LAN constructed in a physical star topology is resistant to failure; downed stations and link failures have minimal effect on the overall operation of the network. The topology allows for simple and economical moves, adds, and changes. It is easy to maintain, monitor, and manage because of the centralized aspect of the topology.

Routing all information through a central point, the hub, has a disadvantage. If the hub fails to function properly, the whole LAN could be affected. Reliability can be increased by dual homing each station to two separate hubs or using hubs with no internal single point of failure.

One example of the star topology is ISO/IEC 8802-3 Ethernet using 10BaseT.

Ring

The ring topology consists of a cable in the form of a ring with stations attached to it, as shown in figure 2-7. A signal

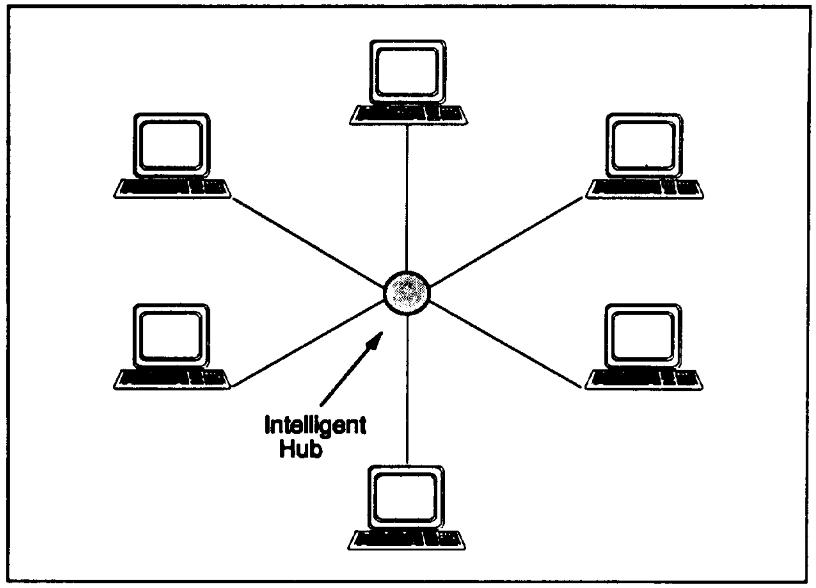


FIGURE 2-6. Star topology.

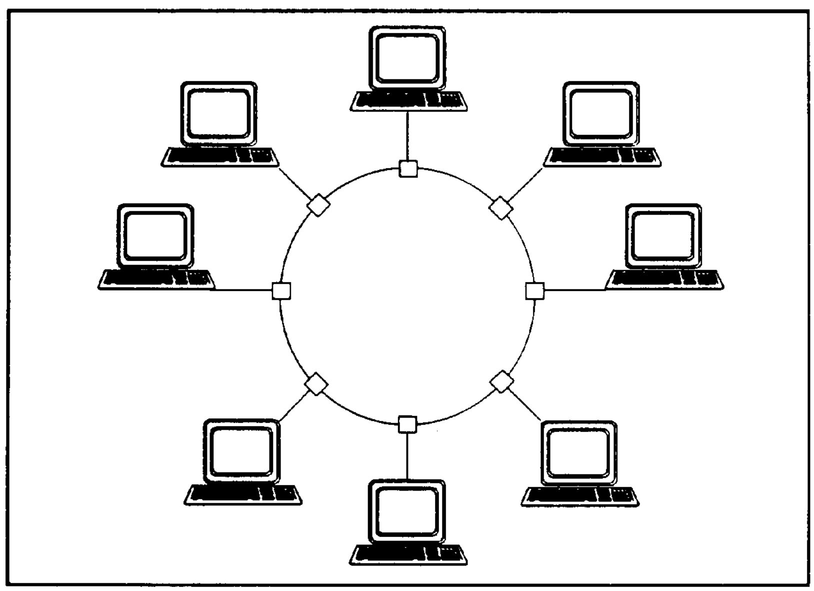


FIGURE 2-7. Ring topology.

is received) regenerated, and retransmitted by consecutive stations on the ring until it reaches its destination address.

If the transmission medium of a basic ring network breaks, the entire LAN goes down. Unlike the bus topology, powering down a station on most ring networks will also disrupt the network. For this reason, all modern ring oriented LANS implement a dual ring, with ring wrap around lost connections.

Moves, additions, and deletions in the majority of LANs with a physical ring topology require bringing the network down until all changes are complete and a viable ring architecture has been restored.

Fiber distributed data interface (FDDI) is a prime example of a ring topology. It avoids the problems inherent in a basic ring topology with a dual-ring architecture (primary and backup ring). Another example is ISO/IEC 8802-5, Token Ring.

Physical vs. logical topology

Figures 2-8 and 2-9 show how the physical and logical layout of a single LAN can differ within a single network.

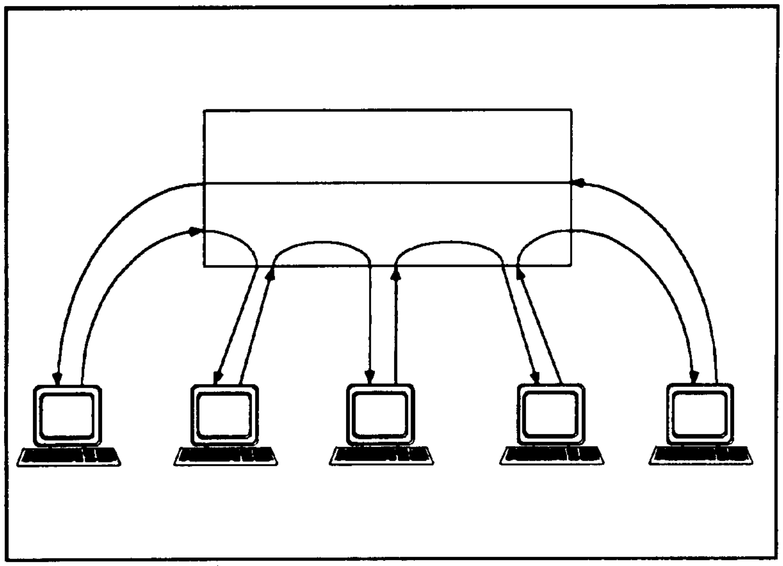


FIGURE 2-8. Logical ring/physical star topology.

In a physical star topology with a logical ring (such as an FDDI intelligent hub), as shown in figure 2-8, stations are independently connected to a central connection point. Outwardly, the LAN appears as a star, but the actual path which the data travels in is a ring.

If the observer does not look at the data flow internal to the central point-of-connectivity in figure 2-9, the LAN would appear to be the same as in figure 2-8. The internal information flow is different though; rather than being propagated like in a ring topology, data is handled as described for a bus topology. The logical bus topology in figure 2-9 is used for Ethernet intelligent hubs.

Both topologies occur in hubs, the logical bus/physical star with 10BaseT modules and the logical ring/physical star with FDDI modules.

Logical LAN configurations based on ring topologies are often implemented as physical stars to eliminate the possibility of failures characteristic of the physical ring

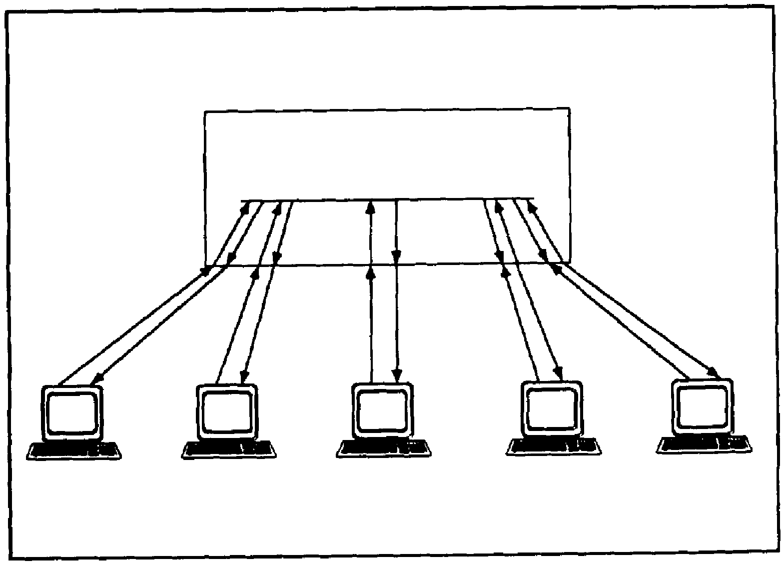


FIGURE 2-9. Logical bus/physical star topology.

topology (for example, the ring breaks due to a downed station).

Another method used to avoid failures is the physical dual-ring architecture. This architecture is discussed in the section that addresses the MAC method of token-passing.

Media Access Control (MAC)

MAC is a sublayer of the OSI data-link layer. The MAC sublayer defines which media access techniques are used to access shared physical media.

For each logical topology to successfully transmit and receive signals across a LAN, rules are required to mediate the right to transmit onto the network. The MAC sublayer determines how information gets on and crosses the LAN.

The two principal methods for MAC, as defined in the OSI reference model, are Carrier Sense Multiple Access/Collision Detection (CSMA/CD) for logical bus topologies and token passing for logical ring topologies.

CSMA/CD

In CSMA/CD, each station is attached to the LAN via a transceiver. Each station is able to listen to the activity on the network. when the network is quiet, a station wishing to transmit does so. In the event that two or more stations make the decision to transmit simultaneously, a collision may occur. Sending stations involved in a collision back off for a random time period and then send again. Each station repeats this scenario until messages are successfully transmitted. As network activity increases, collisions become an unavoidable obstacle to data transmission. Consequently, a CSMA/CD LAN provides a slower response time as the traffic load increases.

Ethernet

A well known LAN architecture which uses the CSMA/CD media access method is Ethernet. GOSIP specifies ISO/IEC 8802-3 as the standard for Ethernet.

ISO/IEC 8802-3 recognizes five media specific standards that govern Ethernet LANs: 10Base2, 10Base5, 10BaseT, Vendor-Independent Fiber-Optic Inter-Repeater Link (FOIRL), and 10BaseF (Draft). The 10 denotes a signaling speed of 10 Mbps. Base denotes that a baseband signaling scheme (Manchester-encoding) is used for data transmission on the network.

10Base5/ Thicknet

10Base5 is ISO’s specification for running Ethernet over thick coaxial cable, with N-Series (or N Type) threaded connectors. 10Base5 is often referred to as Thicknet. The 5 denotes a maximum segment length of 500 meters. 10Base5 specifies a maximum network span of 2.5 kilometers (km) using a backbone transmission path consisting of five segments, interconnected by four repeaters or hubs; three of the five segments can be populated with nodes (stations), and two are Inter-Repeater Link segments (used extending the area the LAN covers). A maximum number of 100 stations/DTEs can be used per segment, with an incremental station/DTE spacing of 2.5 meters, a cable diameter of 0.4 inches, and a maximum AUI cable length of 50 meters.

10Base2/ Thinnet

10Base2 is ISO's specification for Ethernet over thin coaxial cable, usually RG-58 A/U (stranded tinned core), 50 ohm, with standard BNC connectors at either end. 10Base2 is often referred to as Thinnet. The 2 denotes a maximum segment length of 185 meters, rounded to 2 hundreds of meters. 10Base2 specifies a maximum network span of 925 meters (a backbone transmission path consisting of five segments, interconnected by four repeaters (or hubs). Three of the five segments can be populated with nodes (stations), and two are Inter-Repeater Link segments (used for extending the area the LAN covers). A maximum number of 30 stations/data terminal equipment (DTE) can be used on each segment, with an incremental station/DTE spacing of 0.5 meters, a cable diameter of 0.25 inches, and a maximum attachment unit interface (AUI) cable length of 50 meters.

10BaseT

10BaseT is ISO's specification for Ethernet over UTP (4 twisted-pairs per LAN user) in a physical star topology. 10BaseT specifies Ethernet segments (arm of star) up to 100 meters (with only one transceiver per segment), using typical telephone punch down blocks and a modular 8-position RJ-45 connector.

FOIRL

The de facto FOIRL standard specifies a 10 Mbps communication link consisting of two fiber optic strands (transmit and receive) between two Ethernet fiber optic repeater devices. FOIRL specifies a maximum link of 1 km. In this LAN design guide, the fiber link is used for hub-to-hub interconnection and LAN-to-hub connections. The FOIRL standard is an amendment to the 802.3 standard.

10BaseF

10BaseF is ISO's draft specification for Ethernet over fiber optic cable so fiber can be used as a LAN backbone solution. Like 10BaseT, 10BaseF is a physical star topology, and provides the attributes of such a topology. It defines three new and different specifications, 10Base-FL (which modifies an old one, FOIRL), 10Base-FB, and I 10Base-FP. I 10Base-FL specifies a repeater-to-desktop link; I 10Base-FB specifies a backbone or repeater-to-repeater link;

10Base-FP specifies a passive optical link connection, based on a star coupler device. FOIRL modifications support an upgrade to repeater-only FOIRL to include support for stations/DTEs. The maximum segment length for both 10Base-FB and 10Base-FL is 2 km. The maximum segment length for 10Base-FP is 1 km.

Token-passing

In a token-passing LAN, media access is facilitated by a token which is consecutively passed from station to station around a logical ring topology, as shown in figure 2-10, according to a predetermined algorithm.

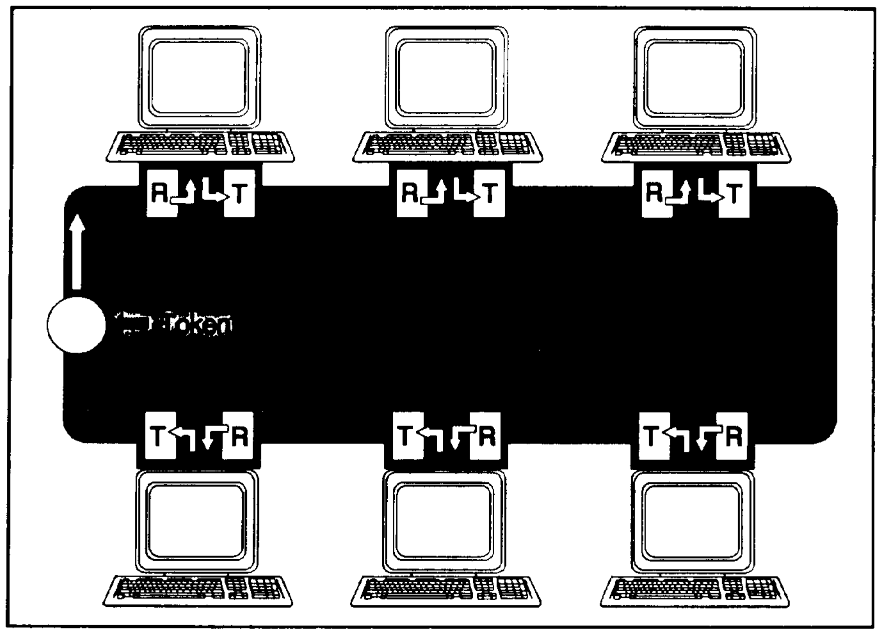


FIGURE 2-10. Token-passing ring.

The token itself is a specialized data stream. It indicates which station is currently in control of the network medium. A station that has possession of the token may transmit on the network. After the token is passed to the next station connected to the network, the right to transmit is given up and the station must wait for the token to make the full circle of the network.

FDDI

A LAN architecture which uses a form of token passing is the FDDI. The FDDI structure is based on a set of dual, counter-rotating rings as shown in figure 2-11.

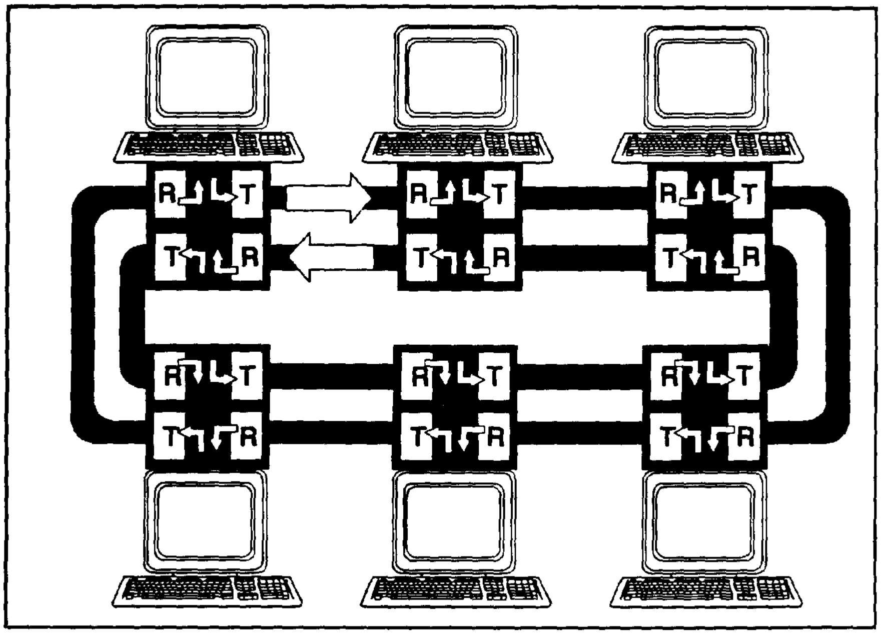


FIGURE 2-11. FDDI dual ring.

In normal operation, only the primary ring carries data. The secondary ring acts as a backup to the primary ring. When a point on the primary ring fails, an auto sense mechanism causes a ring wrap (loop back) so that traffic is diverted to the secondary ring. The point-of-failure is removed from the network, as shown in figure 2-12.

Only stations with a dual-attachment (connection to both the primary and secondary rings) tolerate this type of failure.

FDDI is a high-bandwidth data transmission standard for OSI layers 1 and 2. It is useful for mission-critical LANs and bandwidth-intensive applications. The main reason for FDDI use is its high data rate, 100+ Mbps. FDDI serves as a backbone to LANs. FDDI building backbones reduce the

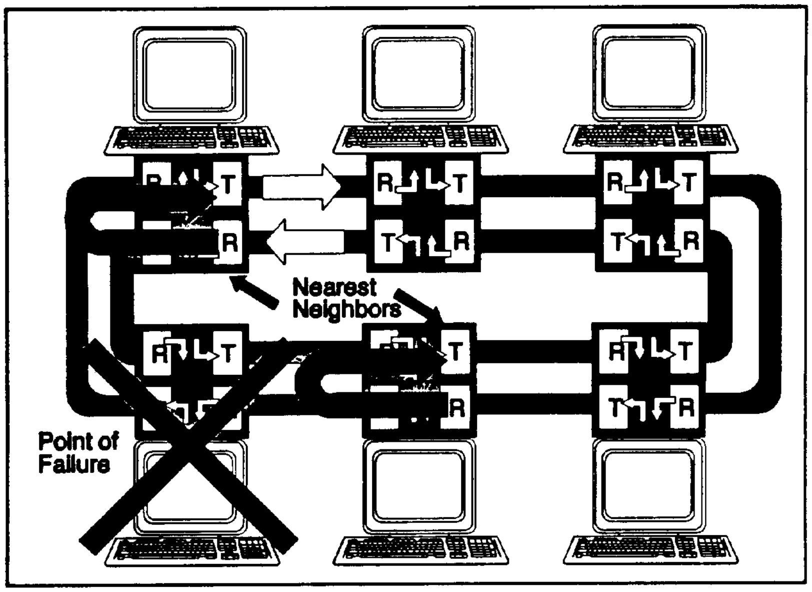


FIGURE 2-12. Point-of-failure on a dual FDDI ring.

need for multiple backbones or segmentation of existing LANs.

Without the use of dual-attachment, an FDDI ring can support up to 2000 individual connections. For every dual-attached station added to the network, the total number of possible connections decreases by one. As an example, if the FDDI ring were to be populated with all dual-attached stations, the total number of connections possible would drop from 2000 to 1000. The FDDI standard (ANSI X3T9.5) specifies that the ring may span a circumference of up to 200 km (100 km for dual rings). The distance between two nodes on an FDDI LAN cannot exceed 2 km. ANSI X3.166/ISO 9314-3, the Physical Medium Dependant (PM D) portion of ANSI X3T9.5, specifies the fiber cable as 62.5/125 core/clad multimode, graded index, 500 Megahertz (MHZ)-km, and 1.0 decibel (dB) per kilometer at 1300 nanometers (nm). ANSI X3.184, the draft Single-Mode Fiber (SMF)-PMD portion of ANSI X3T9.5, specifies single-mode fiber as the transmission medium. FDDI single-mode fiber will support distances of 40 to 100 km between nodes, depending on the network topology.

Transmission media

The transmission medium used in the LAN may be one or more of three basic mediums available: copper cable, fiber optic cable, and free space wireless. Copper cable is the medium used in most LANs today for device connection and the transmission of encoded signals. The wireless technology is still in the developmental stage, although off-the-shelf solutions are available. Fiber optic cable is the medium used for high bandwidth applications.

Copper cable

There are two types of copper cable, coaxial and twisted-pair.

Coaxial cable

Coaxial cable, often referred to as coax, was the first predominant medium for data transmission.

Coax cable consists of two cylindrical conductors with a common axis, separated by a dielectric. As shown in figure 2-13, there are four parts to coaxial cable: the inner conductor, the insulation around the solid inner conductor (the dielectric), a braided wire or metal foil outer conductor which serves as a shield against elector-magnetic interference/radio frequency interference (EMI/RFI), and an outer plastic jacket.

The size of coaxial cable varies. The RG of the cable is usually printed on the jacket of the cable for easy identification. RG is the military identification for the size and electrical characteristics of coaxial cable.

Connectors used with the RG-58/59 coaxial cable are called BNC connectors. These connectors use a "half-twist" locking shell to attach the connector to its mate.

Coaxial cable is relatively immune to EMI/RFI and is able to carry' signals over a significant distance. Coax most often supports a bus topology. It is difficult and costly to install because of its bulky nature. As a result, coax is no longer the most commonly used medium for new installations.

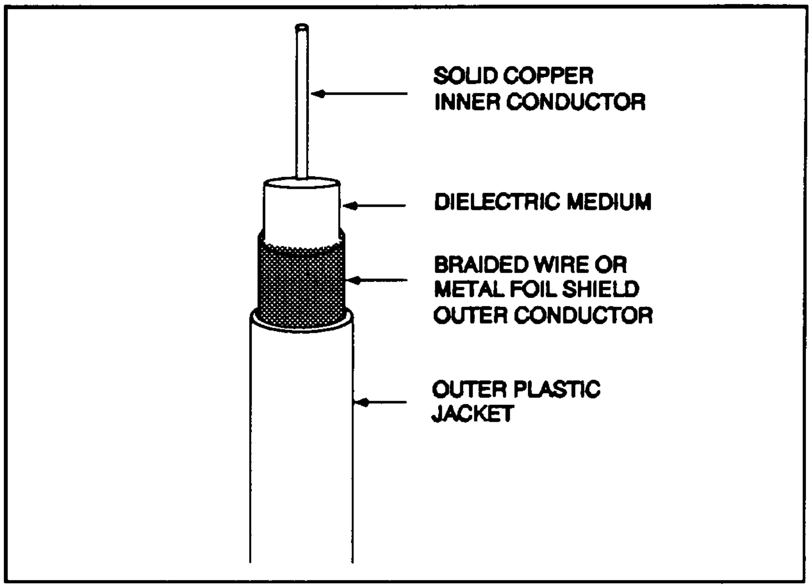


FIGURE 2-13. Coaxial cable.

Coax has a higher bandwidth than twisted-pair and a lower bandwidth than fiber.

Twisted-pair

Twisted-pair cable is the type of cable used in houses and buildings for telephone connectivity to the telephone network. Twisted-pair cable consists of one or more twisted-pairs of sheathed wire, as shown in figure 2-14. The pair is twisted so that the electrical field around one conductor will be as nearly cancelled as possible by the equal but opposite (balanced) electrical field around the other conductor. This reduces the interference emitted by the pair and, reciprocally, reduces the interference by the pair's susceptibility to external fields.

There are two versions of the twisted-pair cable: UTP and shielded twisted-pair (STP). STP has a metallic braid or foil wrapped around the twisted-pairs of wires to provide shielding from EMI/RFI, thus giving it a higher immunity to interference than UTP.

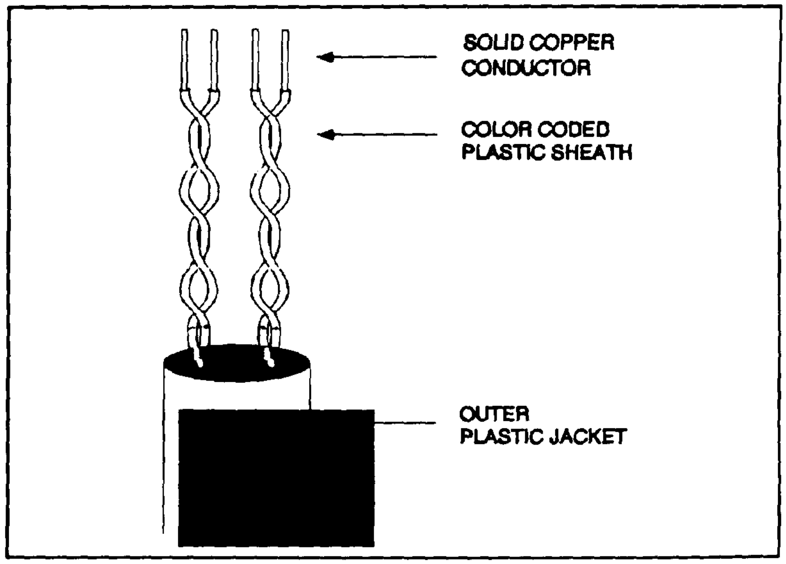


FIGURE 2-14. Twisted-pair cable.

Due to its shielding, STP has a lower bandwidth and higher attenuation than that of a comparable sample of UTP. Therefore, STP is less susceptible to interference than UTP, but UTP of the same gauge can be run longer distances. Also, STP is more expensive than UTP.

The conductor thickness for UTP is usually American Wire Gauge (AWG) 24 or 26; the thickness of STP is normally AWG 22. The characteristic impedance is typically 100 ohms for UTP and 150 ohms for STP.

UTP has become the most commonly used medium for LANs because of its low cost and ease of installation.

Twisted-pair wire uses a small plastic RJ-45 connector. The RJ-45 is an 8-pin connector used primarily for data transmission over twisted-pair wire similar to telephone wire. An RJ-45 connector is depicted in figure 2-15.

Twisted-pair is frequently used for station connectivity to the backbone because it is inexpensive and easy to install compared to coaxial or fiber optic cable. Twisted-pair can be

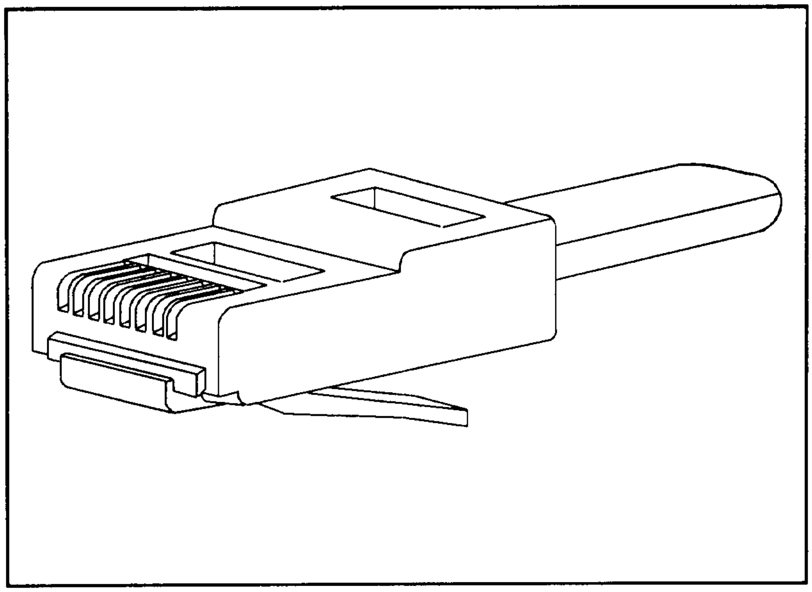


FIGURE 2-15. RJ-45 connector.

pulled around corners, whereas coax and fiber require extra care during installation.

Twisted-pair cable does not offer the bandwidth or distance of either coax or fiber optic cable. Of the three types of cable (i.e. coax, twisted-pair, and fiber), twisted-pair is most susceptible to interference and should not be used in environments where substantial EMI/RFI exists.

Fiber optic cable

An optical fiber is a thin strand of glass or plastic. The higher performance fibers are made of glass. Communication in fiber optics is based upon encoded pulses of light. Each pulse of light is inserted at one end of the glass/plastic fiber by a light source (i.e., laser, light emitting diode (LED)). After traveling the length of the fiber, the light appearing at the opposite end is received by a light detector. The light source and detector are located within transceivers, each interfacing with an electrical medium.

As shown in figure 2-16, the core of the fiber (where the light signal travels) is surrounded by a cladding with an index of refraction less than that of the core to ensure total internal reflection of light.

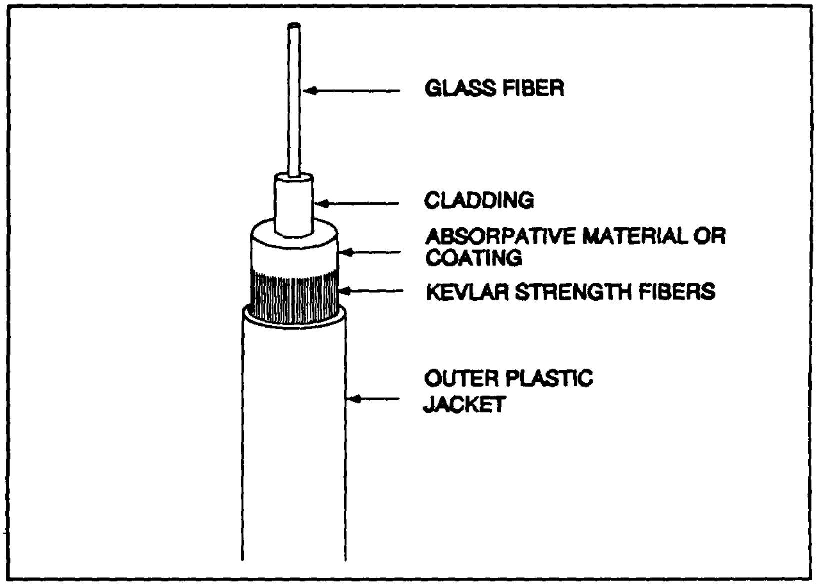


FIGURE 2-16. Fiber optic cable.

The core and cladding are actually a single piece of glass; if the fiber is disassembled, the cladding cannot be separated from the core. The fiber core and cladding are covered by an absorbent material or coating to isolate the inner core from surrounding fibers. Fiber optic cables either have steel or composite stress members mixed with the fibers or a sheath of Kevlar to add tensile strength. This relieves the fibers of stress which results from pulling the cable during installation. (Note: Bending of the fiber attenuates light signals, may cause light to escape from the fiber, and can actually fracture the fiber, breaking the transmission path.) Finally, a jacket covers the entire cable. There is usually more than one fiber in a single cable. Often fibers are grouped with a number of twisted-pair copper wires in what is called a composite cable.

Fiber has a high bandwidth and a low signal attenuation in comparison to coax and twisted-pair; it transfers information at a high data rate with little signal degradation. Because the signals are pulses of light, optical fiber is totally immune to EMI/RFI. Fiber is generally preferred for backbone connectivity between floors or buildings because of the advantages offered by the medium in performance, distance, reliability, and signal integrity.

Optical fiber is a more secure medium than either copper or wireless. To extract data from the medium, an intruder must tap into the fiber somewhere between the optical transmitter and receiver. Once this happens, the intensity of light at the intended destination decreases. Thus, the intruder is easily detected.

In the case of a lighting strike, fiber will not conduct current (unless the sheath has steel members in it).

There are three kinds of fiber: multimode step index fiber, multimode graded index fiber, and single-mode step index fiber.

Multimode step index

In a step index fiber, the index of refraction is constant throughout the glass, and sharply falls at the perimeter of the fiber, where the cladding starts. Thus, light entering the fiber travels in a straight line until it strikes the core/cladding boundary, at which point it is reflected back into the core of the fiber. Light bounces from wall-to-wall of the fiber as it travels towards its destination. Multimode step index fiber has a particularly wide core diameter (common core widths are 50, 62.5, 85, and 100 microns); thus, light enters the fiber at more than one angle. Because of the different angles of entry, light reflects off of the core/cladding boundary at different angles, resulting in multiple paths or modes, as shown in figure 2-17.

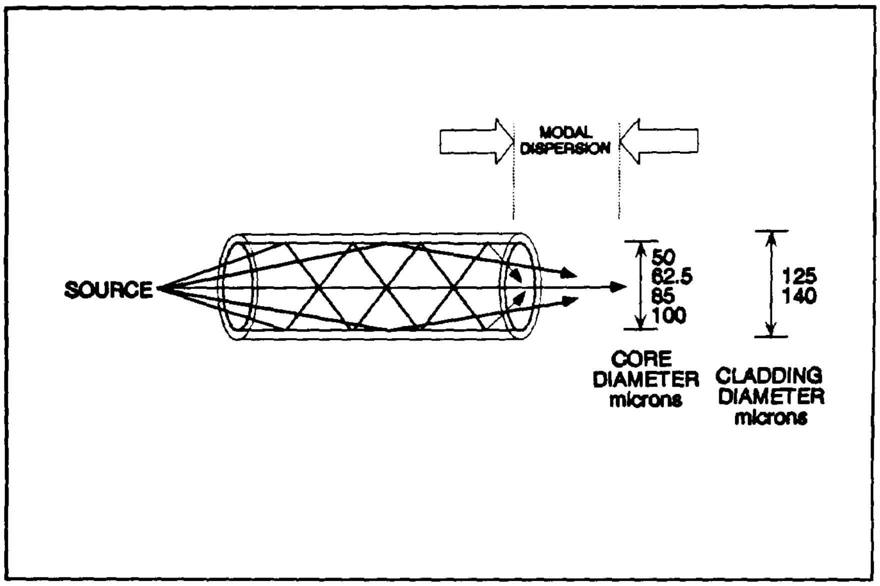


FIGURE 2-17. Multi-mode step index fiber.

The distance light travels in each mode is not the same therefore, not all light arrives at the destination at the same time. This results in “modal dispersion” causing the once separate pulses of light (at the point of entry into the fiber) to be smeared together at the receiving end.

Multimode step index fiber is not recommended for use in LANs, and is not specified in any of the ISO/IEC standards.

Multimode graded index

Multimode graded index fiber allows multiple modes/paths of propagation like the multimode step index fiber. But whereas the step index fiber has a constant index of refraction, the graded index fiber has a variable index of refraction from the center of the core to the outside wall. Light rays traveling through the graded index fiber, instead of being reflected as in the step index multimode fiber, are bent by the changing index of refraction, as shown in figure 2-18. The variable index of refraction of the fiber speeds up or slows down the rays of light, depending on the angle of entry into the fiber, and as a result, the time of travel between the beginning and

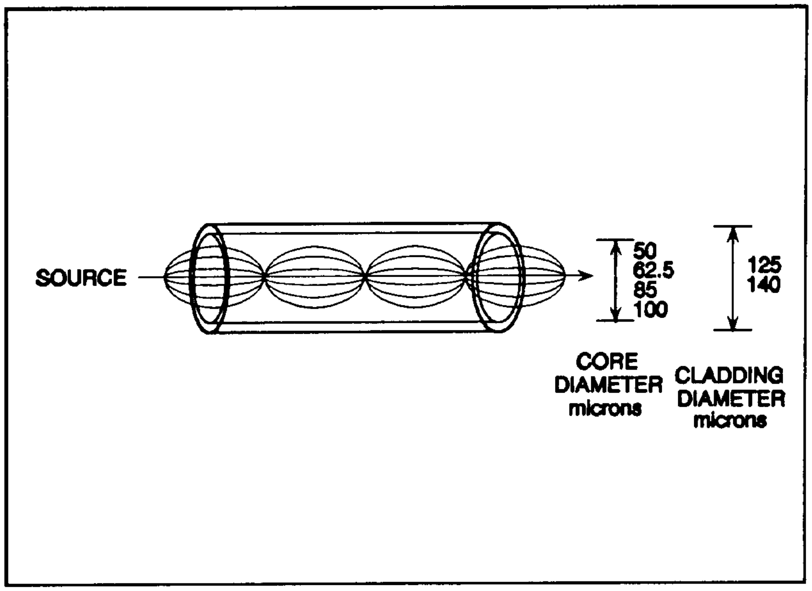


FIGURE 2-18. Multi-mode graded index fiber.

end of the fiber is the same for all signals. Thus, modal dispersion is greatly reduced.

Multimode graded index fiber is used for inside/single-plant applications.

Single-modeode step index

Single-mode step index fiber has a small core diameter, approximately the same size as the wavelength of light, as shown in figure 2-19. Because the fiber is so narrow, light is forced to travel in a single path (single-mode), with no internal reflections, along the axis of the fiber.

Because of the inherent characteristics of single-mode fiber, it can carry a light signal a longer distance than multimode fiber. There are two main reasons. First, even though multimode step index fiber allows more light in initially, the intensity of that light weakens faster due to reflections. Secondly, the modal dispersion inherent in multimode step index fiber, as mentioned earlier, distorts the original signal transmitted. Thus, with single-mode fiber, the signal is stronger and more well defined over a greater distance.

Wireless

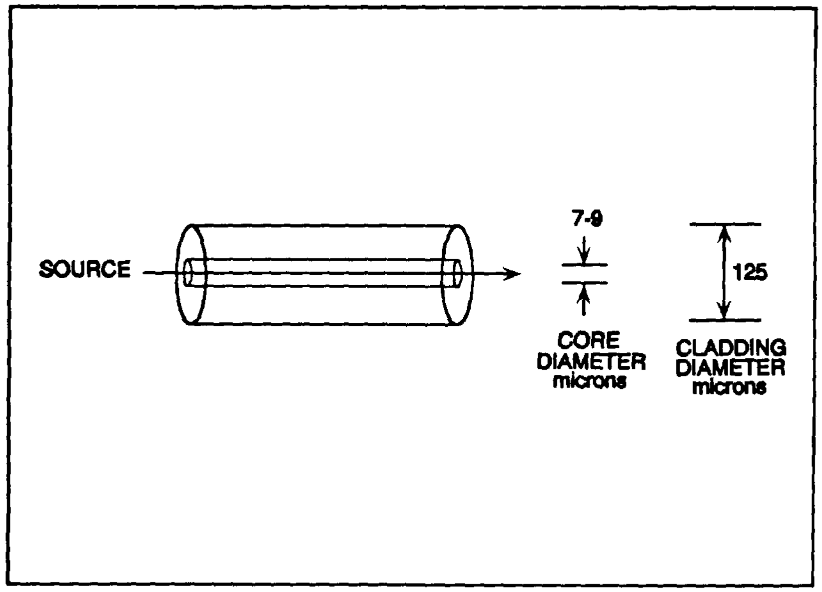


FIGURE 2-19. Single-mode step index fiber.

There are two basic technologies for wireless LANs: radio and infrared light. Radio-based LANs are either conventional (single-frequency) or spread spectrum. Infrared-based LANs are either point-to-point (a focused beam) or broad-beam with up to 360 degrees coverage. Wireless LANs use signal encoding to prevent interference with other LAN users.

Both the radio and light-based LANs are line-of-sight communications. Radio frequencies are degraded, and light frequencies are completely blocked, by walls. Even a person walking between two points of connectivity in an infrared LAN can interfere with a wireless LAN's operation. Besides breaking the line-of-sight, there is always the problem of another wireless product interfering with the wireless LAN (e.g., cellular/cordless phones, garage door openers, home entertainment remote controls, and other wireless networks).

Bandwidth in wireless products is inadequate in many cases; whereas wiring provides dynamic bandwidth, wireless products have a static bandwidth. Also, they can be difficult to install and troubleshoot.

Wireless LANs are often used to support rapid deployment where a temporary set-up is required and low bandwidth can be tolerated. In applications where cable is difficult to install or cannot be run, the wireless LAN may be the only solution.

Currently, there are no standards published for wireless LANs as open systems, and because the technology is still in its infancy, a wireless product purchased today may be obsolete tomorrow.

Radio-based

Radio-based LANs manufactured today are restricted to the industrial, scientific, and medical (ISM) bands (902-928 MHz, 2.4 - 2.5 gigahertz (GHz), and 5.8 - 5.9 GHz). Transmitter power is limited to 1 watt or less. Current radio-based LANs do not require a license for operation under the Federal Communications Commission (FCC)'s Part 15 regulation for unlicensed operation.

Infrared Light

Light frequencies are much higher than radio frequencies; light within the infrared band is invisible to the human eye. Over the years, infrared-light has been the preferred technology for motion sensors and remote controls for televisions and home entertainment centers. Light-based LANs are immune to radio or electrical interference. These frequencies are not allocated by any Government agency, and an operator's license is not required.

CABLE PLANS

Several cabling plans have become de facto standards for cable assembly. As a result, vendors refer to the cabling requirements of a LAN by one or more of the plans. The three plans most often used are the International Business Machines (IBM) Cabling Plan, the Underwriters Laboratories (UL) Data-Transmission Performance Level Marking Program Cabling, and the Electronics Industries Association/ Telephone Industry Association (EIA/TIA) UTP Cable Specifications. Of the three plans listed, only the cable types, levels, and categories applicable to LANs are addressed in this guide.

Type cable plan

A type cable plan is an intrabuilding wiring scheme designed primarily to support the interconnection of IBM equipment. It was the first specification for UTP media use above voice frequencies.

The plan classifies types of cable as follows:

- Type 1 Cable: Two shielded twisted-pair used for data transmission.
- Type 2 Cable: Two shielded twisted-pair used for data transmission and four unshielded twisted-pair used for voice communication.
- Type 3 Cable: Four unshielded twisted-pair used for voice or data transmission.
- Type 5 Cable: Two fiber optic strands.
- Type 6 Cable: Two shielded twisted-pair designed for data transmission. Used as a patch or jumper cable in wiring closets or between a wall outlet and device.
- Type 9 Cable: Two shielded twisted-pair (data rate 16 Mbps) used for data transmission.

Category cable plan

The ANSI, EIA, and TIA developed the EIA/TIA Commercial Building Telecommunications Wiring Standard, ANSI/EIA/TIA 568, July 1991, as a guide for wiring commercial buildings for telecommunications. The same EIA/TIA-568 working group later published the EIA/TIA Technical Systems Bulletin (TSB) 36, Additional Cable Specifications for Unshielded Twisted Pair Cables. TSB-36 identifies the requirements for the transmission performance of UTP cables which are used in premises distribution systems.

Requirements in TSB-36 for categories of cable used for data are as follows:

- Category 2 Cable: Low speed data. IBM Cabling System Type 3 media can be considered as EIA/TIA category 2.
- Category 3 Cable: Data. Cable is intended to handle data transmission rates up to 10 Mbps.
- Category 4 Cable: Data. Cable is intended to handle data transmission rates up to 16 Mbps.
- Category 5 Cable: Data. Cable is intended to handle data transmission rates up to 100 Mbps.

Level cable plan

The level cable plan was developed by UL as it expanded its certification program to include 100 ohm, twisted-pair, LAN cable types for the purpose of safety and performance.

UL identifies levels of LAN cable performance as follows:

- Level 1 Cable: Analog and digital voice and low speed data (20 kbps).
- Level 2 Cable: Integrated Services Digital Network (ISDN) and low speed data (4 Mbps), shielded or unshielded. The cable complies with IBM Type 3 media requirements.
- Level 3 Cable: LAN and medium speed data, shielded or unshielded. Level 3 cable complies with requirements for Category 3 cable in the EIA/TIA TSB 36.
- Level 4 Cable: Extended distance LANs, shielded or unshielded. Level 4 requirements are similar to those for Category 4 cable in the EIA/TIA TSB 36.
- Level 5 Cable: High-speed LAN (for example FDDI over UTP, STP), shielded or unshielded. Level 5

requirements are similar to those for Category 5 cable in the EIA/TIA TSB 36.

Signaling method

The signaling method dictates the manner in which raw bits are transferred across a LAN. There are two methods available: baseband signaling and broadband signaling. A baseband signal is the original signal generated for transmission; it is a pure signal. Two common forms of signal manipulation used on the original baseband signal are non-return to zero (NRZ) and Manchester encoding. In contrast, a broadband signal consists of a group of carrier frequencies (channels) each modulated by baseband signals. The signaling method used in the majority of LANs is baseband.

SIGNAL CONDITIONING DEVICES

A signal conditioning device is used when a signal has to be changed for data transmission in order to minimize the effects of noise, to provide secrecy, or to condense data. There are many different conditioning devices, and they are generally application specific. The signal conditioning device of importance to the LAN designer is the modem.

Modem

The modulator/demodulator (modem) is used to convert a digital signal (ones and zeros) into an audio analog signal (300-3000 Hz) so that signals can be sent over a telephone line, as shown in figure 2-20.

In a single application, two modems are required, one at the sending end and one at the receiving end, to convert the analog signal back into a digital signal.

Modems are generally used to establish computer network connections with isolated LAN users and remote networks.

Some modems can automatically dial and answer. Others require that LAN users dial the telephone number of the connecting modem.

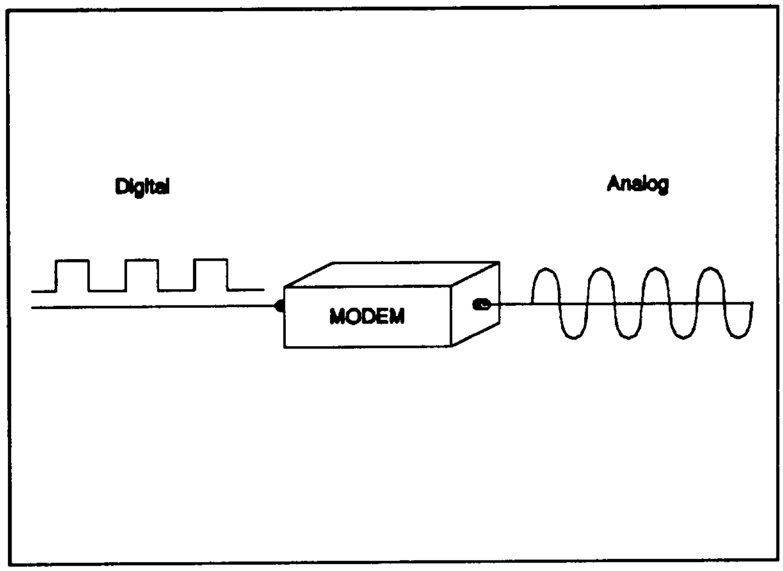


FIGURE 2-20. Modem.

PERIPHERAL DEVICES

A peripheral device is a piece of equipment attached to the LAN. The two most common peripheral devices found on a LAN are the workstation and the printer. According to several magazine surveys, printer sharing is the major reason for LAN purchases today.

Printers

Various types of printers can be used on a LAN. Laser printers are fast, heavy duty, feature-laden devices. They lend themselves to LAN environments because of speed and versatility. Their shared use by many LAN users helps to defray their higher cost. Dot matrix printers are excellent for preprinted forms, multipara forms, and address labels.

Workstations

The workstation represents a node where the LAN user can perform routine tasks such as running software applications, accessing E-mail, and interacting with other nodes.

Minimum requirements for a workstation on the LAN are as follows:

- At least 640 kilobytes of random access memory (RAM)

- A network interface card (NIC) with an address different than others on the LAN

- A disk drive to boot the operating system and run the workstation software.

Network Adapter

For each peripheral device, a network adapter is required. Network adapters are the cards that fit inside a peripheral device on a LAN and implement layers 1 and 2 of the OSI model. The network adapter is the module that connects the network device to the transmission medium. The network adapter is usually referred to as a NIC. The NIC contains the MAC address, usually preset by the manufacturer and unchangeable. Blocks of MAC addresses are issued to manufacturers to ensure that these preset addresses are unique.

Network adapters perform the following specialized functions:

- Provide the interface to drive the signal onto the network media and receive the signal from the network

- Provide the encoding and decoding of the signal.

POWER SOURCE

Power failures, brownouts, and alternating current (ac) power surges and sags can create major problems on computers, LAN systems, and file servers. ANSI lists 111/193 volts as the minimum permissible service voltage on a 120/208 volt service. Most computer manufacturers design their equipment to operate in a voltage range of ±10 percent around nominal. In most cases, measuring voltage at the wall socket would show that the voltage is already near or at either extreme of the voltage range; therefore, any fluctuation will exceed the manufacturer's design limitation.

The following paragraphs discuss power protection sources.

Surge suppression

Surge suppression devices are normally used to protect printers and user workstations. These devices provide noise filtering and surge suppression, generally in the form of a power strip. The surge suppression does not provide for brownouts, voltage sags beyond the nominal limit, or complete loss of power.

UPS

An uninterruptible power supply (UPS) is the safest form of protection for the most critical equipment (i.e., servers and hubs). Most UPS manufacturers provide the ability to monitor the power supply of the server/hub. In the event that power transfers to the UPS, the network can be notified via a separate software monitoring program loaded in the server. The UPS comes in two basic types: standby UPS and on-line UPS.

The standby UPS provides power in the event of loss of commercial power. Under normal conditions, it performs no filtering of power other than surge protection for the equipment. The duration of power availability is determined by the equipment load and battery rating. A turn-on delay time does exist between the loss of commercial power and the power supplied by the UPS, and should be considered with the application.

The on-line UPS provides continuous power filtering and regulation to protect against all forms of power fluctuations. In addition, it provides battery backup capabilities. The duration of power availability is determined by the equipment load and battery rating.

SERVERS, SOFTWARE DRIVERS, AND OPERATING SYSTEMS

Network-attached devices require several types of software to interface with the LAN. These include servers, software drivers, and operating systems (OS).

A server is a computer containing a software process or group of processes working together for the same service goal. Servers are generally high performance workstations or minicomputers such as the 386/486 Intel processor, reduced instruction set computer (RISC) based processors, the 68030/68040 Motorola processors, UNIX based minicomputers, and Digital Equipment Corporation (DEC) MicroVaxs.

There are different types of servers: file, print, network application, database, fax, communication, E-mail, and terminal servers. A file server performs functions such as open, close, read, and write for file resources stored on a departmental LAN hard disk. Print servers provide spooling and centralized print queue management. A print server allows LAN users to quickly transfer print jobs and continue their work without having to wait for free time on the printer. There are printers currently on the market with their own network adapters which eliminate the need for a dedicated print server. Application and database servers store programs and data on a centralized computer so that they can be shared by many users. They also run the programs for users with workstations too small or slow to efficiently run the programs. Communication and fax servers handle dial-up modem and direct-connect remote user connections to the LAN. An E-mail server handles mail storage and transfer on the LAN. Terminal servers provide input/output connection to the LAN for (dumb) terminals.

In smaller networks, several server functions are generally located on a single machine. As a network increases in size, the distribution of server software across the network increases. Normally, a computer used for server purposes contains only the server software and is not used as a workstation because of the large RAM requirement by the server process.

A software driver is the software interface between a network-attached device and the LAN’s transport and operational software. The software driver software is usually installed in or delivered with the NIC. Driver protocols span portions of layers 2 and 3 of the OSI model. The software driver performs frame formatting, error checking, addressing, and other functions to ensure accurate data transmission between network-attached devices. Software drivers are designed for the NIC on which they run. Buyers and designers need to be aware of this fact when ordering NIC cards or driver software.

The Network Driver Interface Specification (NDIS), developed by Microsoft, is one example of a software driver and driver interface for network adapter cards. A second example is Novell's Open Data-link Interface (ODI). ODI is primarily used when multiple protocols must by supported. ODI drivers are not as widely accepted as NDIS drivers. Both of these are standardized and compatible with many network operating systems (NOS) and are available to run on most NIC cards.

OSs are the software that manage the resources of a single workstation. Resources may include the local file system, the memory in the computer, loading and execution of application programs that run in the computers memory, input/output to peripheral devices directly attached to the workstation including NIC, and central processing unit (CPU) scheduling among applications.

NETWORK OPERATING SYSTEMS

Besides the LAN infrastructure (networking devices and cabling), network software is required to organize and manage the network and its users. Computer networking software, or the NOS, oversees the operation of a LAN, coordinating workflow on the network. In the same way that a PC will not operate without an OS, a LAN will not function without a NOS. The NOS is a master control program that controls and simplifies user access to server functions, translates simple names or identifiers into network physical addresses, and monitors network operation. The NOS is the network's software interface between gateways and bridges for integration with other computer environments.

The NOS removes the end user from the complexities of network hardware and software operation of the LAN. Operating in the background, the NOS is transparent to the user. Resources appear as if they are tied directly to the user's computer, when actually they may be located on another floor or in another building.

There are two types of NOS. The basic NOS functions at the network level only, sending and receiving messages across the LAN. It avoids network-attached device control and management. Such a NOS only provides port management and control for the purpose of data transmission. Control includes some form of logon procedure. The more advanced NOSs support the upper levels of the OSI reference model (4-7). They manage input/output (I/O) devices, multiple-concurrent server operations, data storage devices, workstations, and related software processes attached to and on the LAN and provide simpler user interface to these resources.

The NOS runs in the network server. With larger, more complex LANs, the NOS will tend to be more distributed, running on several servers throughout the network. Normally the file and application servers are located on the same server as the network server and are purchased as a package with the NOS. With distributed servers comes flexibility, but also increased maintenance.

Several examples of NOSs are: NetWare, manufactured by Novell; 3Plus Open, manufactured by 3COM; Vines, manufactured by Banyan which runs under the UNIX operating system; DECnet, created by DEC; and TOPS, designed by Sun.

Peer-to-Peer vs. Client Server

The two basic forms of a NOS are the peer-to-peer architecture and the client/server architecture.

In a peer-to-peer environment, the NOS is distributed equally among all nodes (workstations). The NOS enables peer workstations to share printers and files stored on hard drives of other peer workstations, as shown in figure 2-21. Information is sent over the cabling system without the need for a dedicated server. A pure peer-to-peer NOS can only effectively support a limited number of concurrent LAN users.

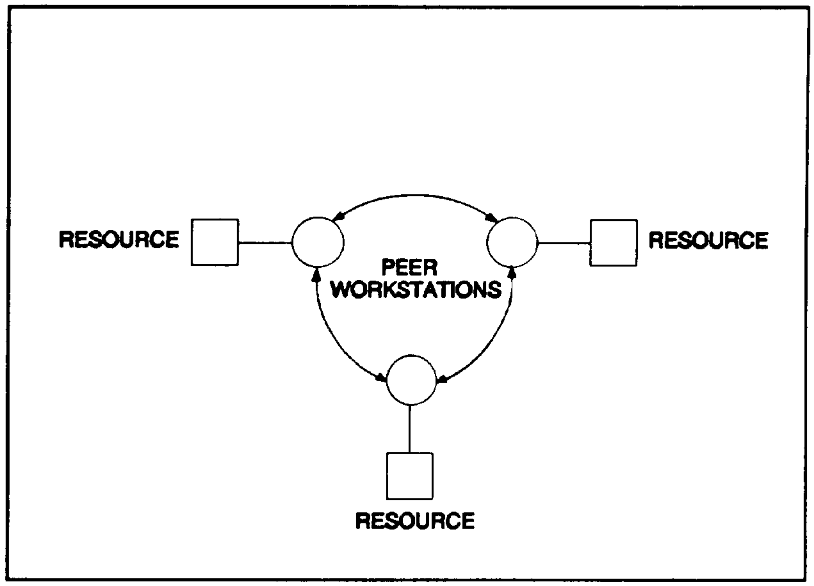


FIGURE 2-21. Peer-to-peer architecture.

In a client/server arrangement, the major portion, or all of the NOS, runs on a dedicated server (the network server). Applications that make use of the central node (dedicated server) are called clients and run on client workstations, as shown in figure 2-22. For a client workstation to communicate with the server, it must have a small part of the NOS running in it. This software is called a shell or redirector and is responsible for connectivity with the server. The client/server NOS is capable of supporting large numbers of concurrent LAN users, but is limited by the size and speed of the server running the NOS software.

NetBIOS

Network Basic Input Output System (NetBIOS) is a software process used to interface applications resident on the LAN with the NOS. NetBIOS creates application interfaces between the application and the LAN at the session, transport, and network layers.

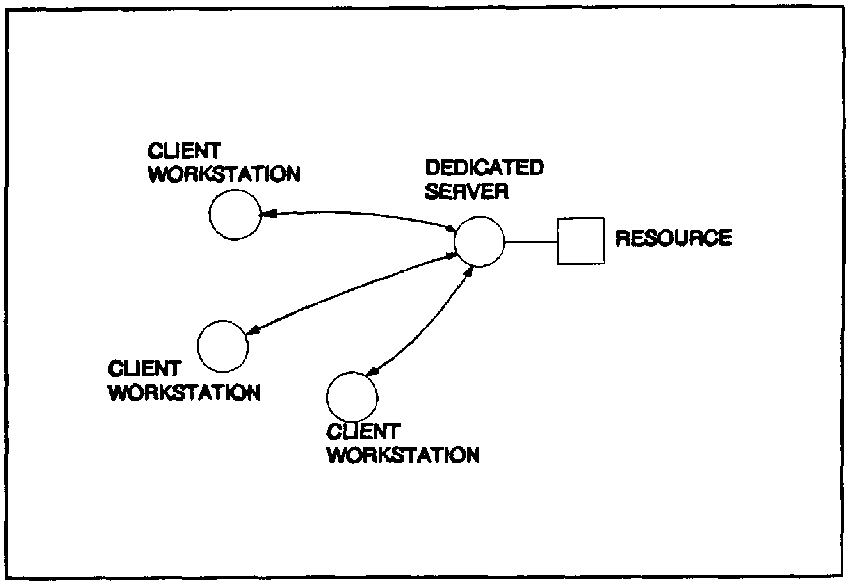


FIGURE 2-22. Client-to-server architecture.

NetBIOS was developed by IBM as a protocol for direct peer-to-peer communications between network-attached devices. The NetBIOS is placed on the IBM PC network adapter. In this framework, the PC does not perform any of the lower level functions. The drawback to locating NetBIOS on the adapter card is that a bottleneck is created on the card. Because of this, a number of NOS vendors emulate NetBIOS on the system and bypass the NetBIOS firmware on the network adapter.

Access Security

The NOS provides a means of creating network login and password features. The NOS allows a network administrator to institute varying levels of security on the network. Thus, the NOS coordinates network access levels for end users, being a delimiter for loading, execution, and use of shared application programs, files, and network devices.

NETWORKING DEVICES

The majority of LANs today are contained within a single building, but are seldom totally isolated from the outside world or isolated from other LANs within the same building.

Instead, LANs, independent of location, are connected by a number of networking devices, such as repeaters, bridges, routers, and gateways, which reconstitute, restore, and synchronize signals flowing between LANs.

Networking devices are used to transfer and regenerate signals over extended distances, so that signal transfer can occur between LANs over vast distances. These devices physically tie networks together in order to move data across network boundaries. Networking devices are the building blocks of the network infrastructure. No single device is best for all applications and, as a result, most large networks include a mixture of devices.

Repeaters

Repeaters extend the distance a signal is normally able to travel on a LAN segment. Placed between two cable segments, the repeater regenerates incoming signals, provides synchronization, and forwards the data on the outgoing cable segment. There can be more than one repeater in a series. Repeaters perform at the physical layer of the OSI model, see figure 2-23.

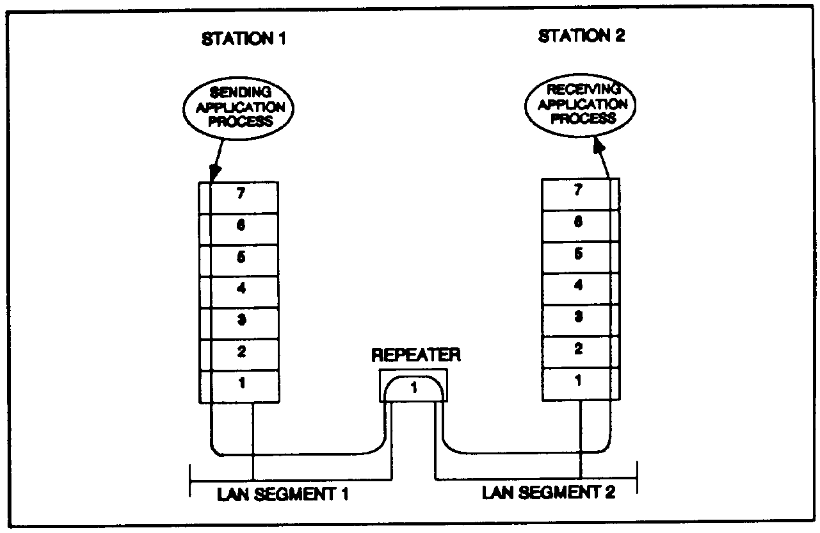


FIGURE 2-23. Repeater.

The main disadvantage of a repeater is that it passes along everything it detects on the line. If there is noise or distortion, the repeater passes it along with the original signal.

There is a limit to the number of repeaters that can be used to extend a LAN's length and topology. In an Ethernet LAN, there can be a maximum of five segments, interconnected by four repeaters.

Bridges

Bridges repeat data between two separate, but similar types of LANs, such as Ethernet or FDDI. The bridge filters the data flow between the LANs, passing only those messages addressed to a destination on the opposite side of the device. The bridge does this by learning the MAC addresses in the LANs attached to it. Bridges perform at layer 2 (data-link) in the MAC sublayer of the OSI model, see figure 2-24.

A bridge cannot make decisions about routes through the network because information on routes is encoded in the network address that is accessible only by the network

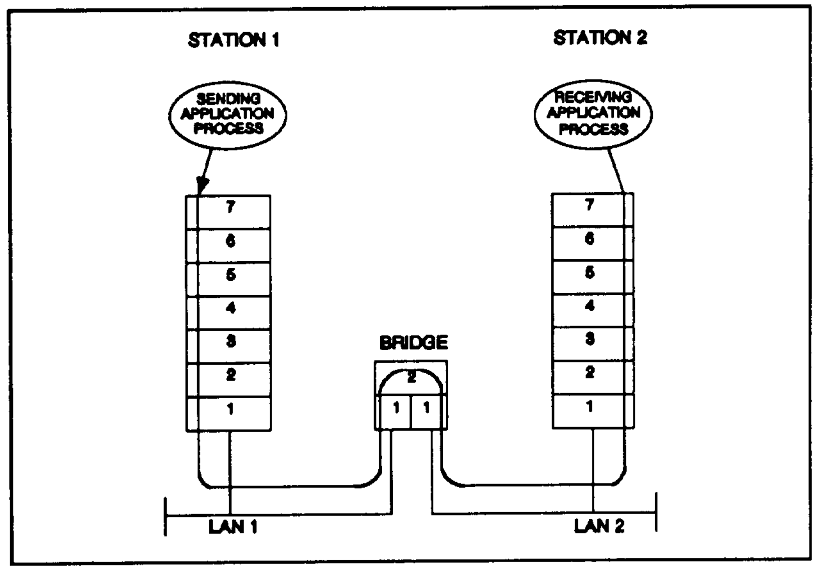


FIGURE 2-24. Bridge.

layer.

Because of its filtering characteristic, the bridge is used not only to extend, but to segment, a LAN. The bridge is a possible solution to a large, overloaded LAN. By breaking such a LAN into segments, the user load can be distributed to make more cost-efficient use of the media without compromising performance.

Bridges can be employed locally or remotely. A single local bridge ties two collocated LANs together. Only one device is necessary. Local bridges operate at LAN transmission speeds (e.g., 1 Mbps, 10 Mbps, and 100 Mbps). Remote bridges connect two distant LANs, see figure 2-25, instituted at both ends of a WAN (i.e., serial link (dedicated or dial-up), X.25 packet network, ISDN, fast packet network providing frame relay service, switched multimegabit data service (SMDS), or asynchronous transfer mode (ATM)/broadband-ISDN (B-ISDN)). Because of the transmission rates they interface with, local bridges are designed to operate at higher speeds than remote bridges (e.g., 56 kbps, T-1 (1.544 Mbps)).

Ethernet Switch/ Ethernet Multiport Bridge

The Ethernet switch and Ethernet multiport bridge are two specialized examples of the bridging device. Because these devices are used to connect multiple Ethernet

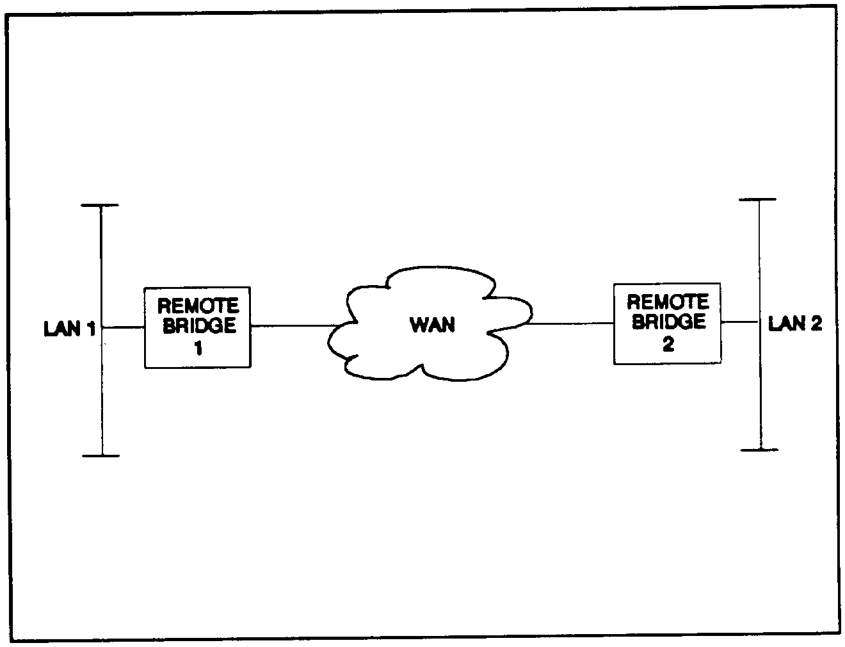


FIGURE 2-25. Remote bridges.

segments and because the technology behind the two bridging devices is a hub, both devices are referred to as multiport bridging hubs.

A multiport bridging hub allows many different computers or LANs (Ethernet segments) to communicate between themselves in an efficient manner. Each port on the hub can transmit or receive information simultaneously, each at the full 10 Mbps rate. The hub will then sort out which incoming packets need to go where, and will only transmit each packet to the port that needs it. It is possible for all ports to be receiving a different packet at the same time, or for all ports to be transmitting a different packet at the same time. The multiport bridging hub transfers the data internally at many times the 10 Mbps rate, allowing for a much faster backbone operation. Multiport bridging hubs are part of a system called a "collapsed backbone," and can be more efficient than a high-speed backbone network for some applications. The multiport bridge would be most useful for a large number of workstations running different compressed video applications. FDDI would be more useful for un-compressed video, high-speed file servers, or other very high-speed data applications.

Routers

Routers repeat data packets between multiple LANs at layer 3 (network) of the OSI model, see figure 2-26. with the transmission capabilities built-in, the router is able to evaluate the network environment (traffic) on a per packet basis to make intelligent routing decisions.

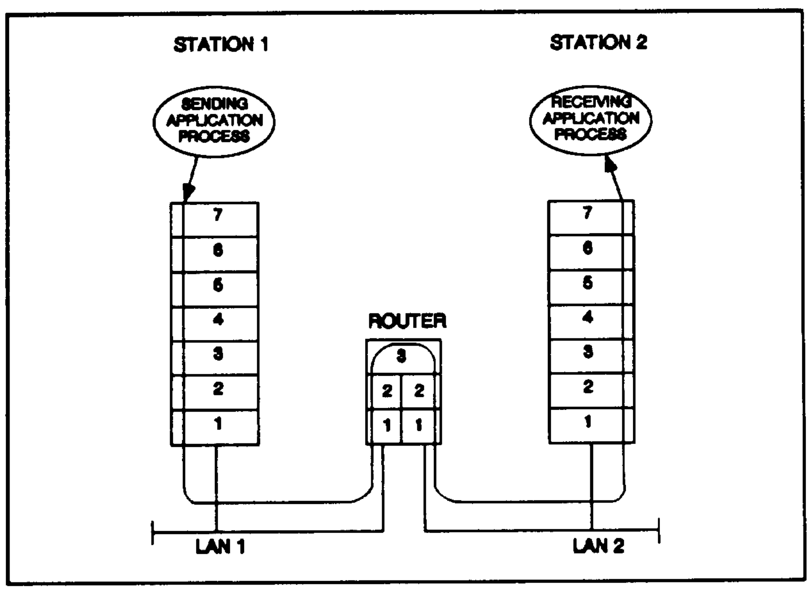


FIGURE 2-26. Router.

Routers are frequently tied to other routers and there may be multiple "hops" between the originating source and final destination. Thus, a signal packet may have to pass through several routers (with multiple pathways) to reach its ultimate destination. In such a case, the intelligence behind the router allows each routing device (along the transmission path of a packet) to identify which path to the destination is best in terms of hop count, congestion, and outages.

Gateways

Gateways mediate communication between networks using incompatible protocols. The device understands the data handling formats of each network it interconnects. Gateways link LANs at the session, presentation, and application layers of the OSI model, see figure 2-27.

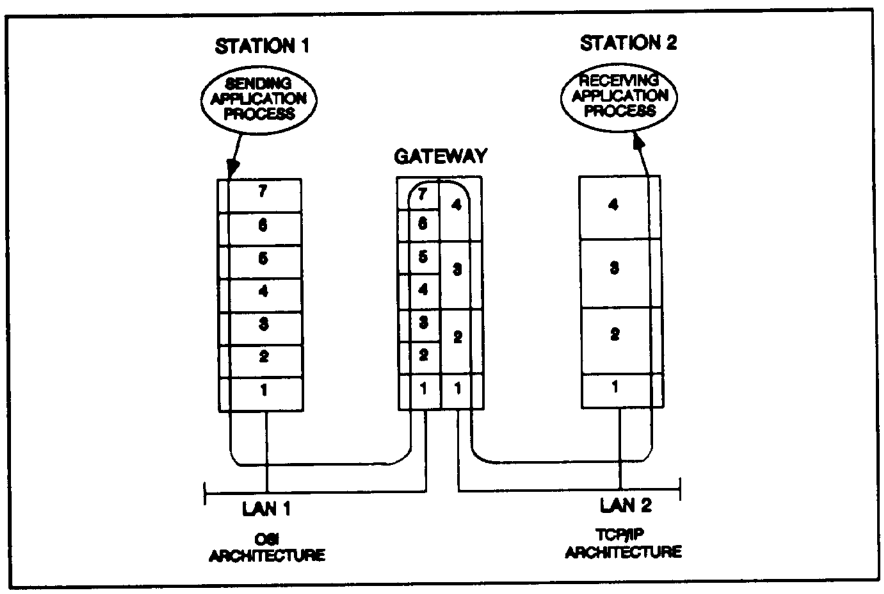


FIGURE 2-27. Data flow between protocol stacks interconnected by a gateway.

Hubs

A hub consists of a metal chassis, an integral backplane, and a standard number of removable modules. Modules consist of I/O modules (such as 10BaseT, 10BaseF, and FDDI) and networking modules (such as bridge, router, power supply, and network management). Each module plugs into the backplane where signals from individual modules are merged. without the networking modules installed, the hub is simply a multiport repeater; incoming signals are repeated across the hub by each 110 module. A typical hub looks like that shown in figure 2-28. with the flexibility of I/O and networking modules, the hub can be configured to meet a wide variety of networking requirements.

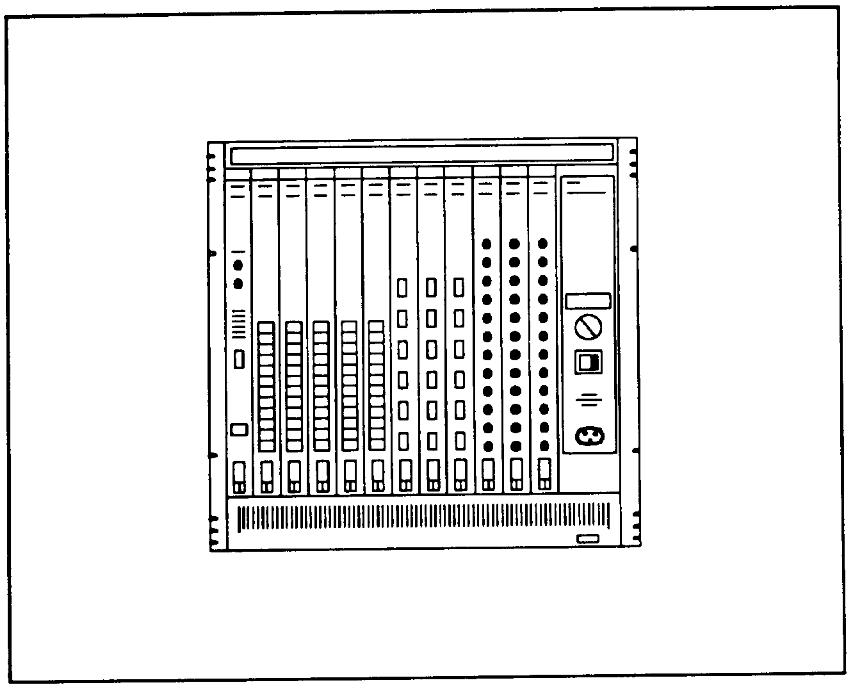


FIGURE 2-28. Hub.

A hub that uses high-speed routing or bridging internally to provide maximum speed to each port is commonly referred to as a collapsed backbone. The collapsed backbone enhances communication and minimizes congestion between LAN segments. The collapsed backbone provides a central point-of-connectivity for LAN segments. The basic idea behind the hub is centralized network connectivity. Hubs are always found in networks using a physical star topology.

INTER-CONNECTIVITY CONSIDERATIONS

In the installation of any LAN device, the interface requirements to existing LANs, gateways, PCS, and mainframes must be considered. Currently, the Army has a conglomeration of physical media, hardware, and access methods. Many different protocols and access methods are being used including Ethernet, token ring, TCP/IP, transmission protocol 4 (TP4), and other vendor specific protocols. With the implementation of gateways, some of these systems can be interfaced with the LAN. However, others are proprietary and do not incorporate the OSI architecture. It will be necessary to contact the appropriate vendor to determine interoperability and to determine the costs of interfacing the proprietary system with the new LAN(s). The physical medium may include coax, twisted pair, and optical fiber.

The Common User Installation Transport Network (CUITN) program will be fielding a backbone network at selected Army installations for interconnection of LANs. However, it is anticipated that it will take over 10 years for this program to be deployed to all identified Army installations. In the interim, the following methods can be used to connect LANs which are in separate buildings or to connect the LAN to the Army gateway.

Via modem

A line driver device or modem (error correction capabilities highly recommended) is used when the connection is to a serial port of the server. The modem device is connected to a line that has a dedicated circuit to another building. At the other building, the line is connected to a second modem which is attached to the serial port of that server. Modems can support user-to-user and network-to-network communication at data rates greater than 1.2 kbps, and up to 14.4 kbps without data compression.

Via bridge

A remote bridge connects on one side to the LAN and on the other side to an intermediate device. The intermediate device depends on the data-link service, for example 56 kbps or TI (1.544 kbps). The bridge connects to a channel service unit/data service unit (CSU/DSU). The CSU provides the physical and electrical termination for the telephone wiring. The CSU is specific to the type of circuit used. The DSU is a serial data port that provides a connection, typically RS-232, RS-449, or V.35, between the CSU and the router/bridge. These devices are described here as individual pieces of equipment; however, the newest bridges often contain internal DSUs. Also, the bridges and CSU can be modules that occupy slots in intelligent hubs.

Via X.25

Another interconnection method is to connect the server in one building with the server in the other building using X.25 packet switching. This requires that X.25 software and the interface software be loaded on both servers. In addition, X.25 (minimum 9600 bits per second (bps)) modems must be purchased. The connection is made through the serial port of one server to an X.25 modem equipped with a packet assembler/disassembler (PAD) through a dedicated line to the receiving building's X.25 modem to the serial connection in the receiving server. The advantage of X.25 is that it provides error correction and flow control. It will allow multiple sessions between servers. Modems that are X.25 meet the international standards. X.25 is also a common protocol between routers in a WAN.

Note:

The PAD prepares the data for transmission between the networks. The PAD connected to the sending server bundles the moving data into packets. The PAD connected to the receiving server unbundles the packets as they arrive. The PAD can either be a part of the modem, a card in the server, included in a router, or a separate device.

Via wireless

Another interconnection method is to incorporate wireless technology. Currently, wireless is not standardized and systems on the market are proprietary. The three technologies used are ultrahigh frequency (UHF), microwave, and infrared light.

EVOLVING TECHNOLOGIES

Important evolving technologies today include ISDN, B-ISDN, synchronous optical network (SONET), and ATM.

ISDN

The ISDN provides universal end-to-end connectivity, usually over digital lines. The technology calls for a complete digitization of telephone systems by converting analog circuits to digital circuits, that is, by circulating zeroes and ones instead of analog frequencies. What is special about the ISDN is that it can be used to move data, voice, image, facsimile, etc., either separately or simultaneously, over a single pair of copper wires. For LANs, this would provide a universal communications network for multimedia communications; networks could simultaneously transfer data, voice, and video over a single WAN (ISDN). The protocols for ISDN appear in layers 1 through 3 of the OSI model.

ISDN can be described in terms of a basic rate interface (BRI) and a primary rate interface (PRI). BRI provides three simultaneous digital channels: two 64 kbps channels (B-channels) plus one 16 kbps channel (D-channel). PRI provides 1.544 Mbps (= twenty-three 64 kbps B-channels and one 64 kbps D-channel).

SONET

SONET is an evolving fiber optic interface and synchronous multiplexing standard. As a solution for implementing high-speed fiber in the public network, SONET provides optical carrier (OC) channel speeds ranging from OC-1 (51 Mbps) to OC-48 (2.4 Gbps). SONET allows new types of service such as B-ISDN, and makes it possible to provide existing services more efficiently. SONET defines a set of physical layer (layer 1) standards.

ATM and B-ISDN

ATM is an evolving specification for concurrently transferring all types of data, including digitized voice, digitized video, data, and LAN signals over a wide range of speeds (i.e., 51 Mbps to 2.4 Gbps and beyond) over long distances. ATM can support real-time (low latency) signals and non real-time (latency independent) signals. ATM itself is a communication protocol that operates at the MAC sublayer of the data-link layer.

ATM can be used in both LAN and WAN environments. It is the first technology which can bridge the gap between these two different technologies.

B-ISDN is a huge fiber optic pipe technology. Based on the SONET standard, B-ISDN is much faster than ISDN. ATM is currently being standardized for use with B-ISDN; SONET is to be used to carry ATM frames.

COMPUTER VIRUS ISSUES

A computer virus is a program that attaches itself to a computer system and causes the system to perform in some abnormal fashion. Viruses are passed from system to system by attaching themselves to software, which is then borrowed or copied. The result of a computer viruses may be as simple as an annoying message, or as catastrophic as the loss of data or an OS.

Networks must be secured from computer viruses from the workstation to the server. As a general rule, the best way to fight virus attacks is to prepare for them.

Virus locations

There are various places in the network where computer viruses may reside on, as well as attack, the network. The following are some of the potential places where a virus may reside.

Executable files

The executable files (.exe, .com, or overlay) are a major vehicle for virus replication. The virus appends to an executable file and executes when the file is executed.

Boot sectors and directories

Boot sector viruses attack the boot sectors of a disk. These virus areas spread throughout the network on floppies and via hard disk. They destroy directories and file allocation tables.

TSR virus

Terminate and Stay Resident (TSR) program viruses usually hide in the PC's memory and infect files by intercepting disk operating system (DOS) interrupts and replicating each time the command interpreter executes, thus using DOS to infect other files. The virus installs in memory and begins to infect still more files. When its trigger condition occurs, it activates and does its damage.

Stealth virus

Many of today's stealth viruses hide in the workstation RAM waiting transfer to the network. The stealth virus avoids detection by knowing how to bypass DOS interrupts, similar to the way the TSR operates.

Virus solutions

Antivirus programs can protect just the network drives; this, however, only resolves half of the viruses. Another solution is to scan files as they travel to and from the workstation, but this only detects parasitic infectors. The next best way is to scan the workstation. This can be done manually, under command from the LAN user or system administrator, or automatically using a TSR in the workstation RAM. The station lock virus checker represents a more effective automatic way of virus protection.

Manual method

The manual method assumes that the system administrator remembers (or has the time) to scan the system or that the LAN user remembers or takes the time.

TSR method

The TSR program virus requires memory. Workstation RAM is always at a premium and TSRs behave badly with certain programs, especially WINDOWS. Most networks apply virus protection in the file server software.

Station lock method

The station lock method does not need to know what a virus is, just what it does. It is based on the concept that a virus must perform limited types of activities to infect the system. For example, one type of virus must intercept a DOS interrupt call, then it must attempt to change the program pointer to point to itself so the virus is executed first. Thus it gains control of the system.

Station lock also addresses some fundamental problems of network security such as access control, unauthorized copy prevention, and workstation resource restriction in a peer-to-peer environment. By watching for these and other activities, station lock can predict virus attacks with virtually no misses or false alarms.

Tips on virus detection

Virus detection can occur by observing how the system responds.

1. Programs used daily are beginning to run more slowly.

2. Disk access appears ill-timed or more frequent than normal.

3. Program load time increases, not just at peak usage times.

4. The microcomputer locks up. Normal lockup is from power, sloppy programs, or hardware incompatibility.

5. Hardware and software problems appear after something new is added to the system.

6. Unusual or humorous error messages appear.

7. Free disk space decreases dramatically.

8. Memory-resident programs execute incorrectly or not at all. Typically found in RAM and intercept DOS calls.

Tips on virus protection

Virus protection amounts to common sense computer practice.

Backup the system regularly, since some viruses lay dormant for weeks, months, or even years before activation.

Purchase a good virus checker which includes scanners that check files for known signatures and monitors that check DOS calls. The checker compares programs by taking snapshots of the disk to use for comparison.

Do not download programs from bulletin boards directly to a network station. Do this only to stand-alone computers.

Do not buy software from unusual vendors, use only government approved sources.

Do not allow others to borrow or use your computer or original program disks.

Make the .com and. exe files read only files.

Teach network users why they must comply with policies regarding file transfer.

Track LAN users who have more difficulty than others and those who abuse the system.

Do not let support people use viruses as a convenient excuse for every problem.

Establish a policy that an observation of irregular behavior (potential computer virus) should be reported immediately to a central network authority and not overlooked. Let a network professional decide whether a problem exists or not. If a virus is detected, all nearby computers at risk should be checked as well. To minimize infections, early reporting should be strongly encouraged.

LAN DEBUGGING

When troubleshooting a LAN failure, it is fairly easy to identify what the symptom is; however, it is more difficult to figure out why the problem exists. LAN diagnostics help isolate the failure and generally consist of one or more of the following actions:

1. Locating damaged physical components

2. Identifying misconfigured devices on the LAN

3. Solving problems reported by LAN users.

Network faults

Network faults can be related to specific levels of the OSI reference model. With respect to the reference model, faults can be divided into two distinct areas: layers 1-3 faults and layers 4-7 faults. Approximately 80 to 85 percent of all LAN problems occur at the transmission layers, and most transmission layer faults are the result of hardware problems. Conversely, 15 to 20 percent of the LAN problems occur at the application layers in software.

For example, layers 1-3 faults in an Ethernet LAN can exist because of:

1. Cable or connector breaks and shorts
2. Bad, faulty, or missing termination
3. Incorrect routing for MAC address
4. Bad NIC/AUI/transceiver
5. Too many repeaters
6. Incorrect network configuration
7. Incorrect station spacing on the backbone
8. Faulty Ethernet controllers
9. Defective software.

The faults mentioned above can result in the following:

1. Excessive collision of packets
2. A high number of error packets
3. Inexplicable "jabber" packets

4. Late collisions

5. High error rate for a specific station

6. Stations that transmit or receive, but cannot do both

7. Timeout delays in packets

8. Specific stations that cannot communicate

9. Total network failure.

To identify problems occurring at layers 1-3, a protocol analyzer with statistical tools is normally used. Such a diagnostic device helps to identify nominal and peak utilization, excessive errors, collision counts, short packets, late collisions, and the number of packets sent and received.

Layers 4-7 problems are typically regarded as software faults. Such faults are for the most part due to software incompatibility and configuration issues such as insufficient buffer management and overloaded servers.

To identify problems occurring at layers 4-7, a protocol analyzer that includes a protocol decoding tool is used. Such a device gives a troubleshooter the ability to decode the information contained in packets traveling across the LAN. In many cases it is the actual application being used which is at fault, not the LAN infrastructure, and the only way to tell this is by decoding the packets generated by the application. Software tools that run on a workstation and allow it to function as a protocol analyzer are available to analyze the configuration of a LAN.

LAN test equipment

Specialized equipment is available for testing interfaces, terminals, modems, transmission lines, and communication software, as well as for monitoring and managing entire networks.

Analog test sets

Analog test sets are invaluable tools for testing networks using twisted-pair facilities. Analog test sets measure phase jitter and phase hits, which create havoc on data circuits that use phase-modulated modems. In addition, they measure phase and amplitude modulation, signal-to-noise ratio, peak-to-average ratio (P/AR), gain hits, frequency, power level, 2- and 4-wire return loss, attenuation, and more. Advanced analog test sets measure the analog characteristics of high-speed facilities including T1, microwave, and satellite links.

Digital test sets

Digital test sets range from relatively simple, handheld interface breakout boxes to bit-level testers to sophisticated programmable devices.

Interface breakout panels

Interface breakout panels are inexpensive, handheld devices that serve the network technician at the lowest level of troubleshooting. The handheld interface breakout panel generally used for an RS-232C interface provides access to the individual pins on the interface for the attachment of test probes from devices such as voltmeters, scopes, or protocol analyzers. This unit is most useful for testing the interface connector or resolving unique intercompatibility problems. In addition, breakout panels function in elementary modem and terminal testing applications to ensure that the signals reaching the interface from the device in question are entirely within specifications.

Data line monitor

The data line monitor connects in series (in-line) between the terminal and modem, allowing the LAN user to see which blocks or characters of data are transmitted incorrectly. Features include "freezing" display on a specified condition or programmable parameters. Actions, routines, sequences, and timing are performed in response to specified conditions when they occur.

DTE/DCE emulators

DTE/data communications equipment (DCE) emulators perform all functions of a monitor and perform interactive tests at the character level. A good emulator verifies that a given device or program fits the specifications of a particular network before actually installing the component in the network. Most emulators simulate and verify data up to the transport layer (layer 4) of the OSI reference model.

Data recorders

Data recorder devices connect in-line to active data connection, trapping certain time-specified faults over a period of time.

Protocol analyzers

The protocol analyzers allow LAN users to monitor specified protocols to detect problems such as software errors, incorrect terminal addressing, and parity errors without disrupting normal network operations. Data can be trapped and stored in a capture buffer for later analysis.

T-carrier testers

The T-carrier tester tests digital signal 1 (DSI)/T1 transmission facilities (either point-to-point applications or backbone networks) that have become a potential liability due to either catastrophic failure or partial impairment of the communications equipment or the line. The tester connects to DSI span line through a CSU or cross-connect point and uses source timing or derived timing from loop timing. Functions of T1 test equipment include:

1. Analyzes framed or unframed DSI data

2. Measures errors, bit error rate (BER), and error free seconds

3. Measures bipolar violations, violation rate occurrences, and violation-free seconds

4. Generates up- and down-loop codes for CSU control

5. Allows testing through the Defense Switch Network (DSN).

Fiber optic testers

The fiber optic testers usually measure loss and power through the fiber. This test equipment is usually classified as Optical Time Domain Reflectometers (OTDRs) or Optical Loss Sets (OLSs).

OTDR

An OTDR analyzes cable integrity by measuring the time required for a lightwave pulse to reflect from a surface such as the cable end or a break in the fiber. The OTDR sends a pulse into the transmission medium and records/displays the pulse's reflection to indicate continuity, discontinuity, lack of integrity, cracks, fractures, breaks, and so forth.

OLS

The OLS is used to test the integrity of an entire fiber circuit based on power loss. It consists of a source (emitter), placed at one end of the circuit, and a detector (power meter), placed at the other end. A loss test measures optical attenuation (in decibels) between two points in an optical path.

SECTION 3. LAN DESIGN PROCESS

DESIGN PROCESS OUTLINE AND LAN DESIGN FEATURES

GENERAL

This section presents an outline of the LAN design process, describes features common to all LANs designed using this process, and defines four LAN design performance variations generated within the design process. The remainder of section 3 outlines the steps for designing a LAN of any size, from 50 to 1000 users, and for selecting one of the four performance variations for the final LAN design.

LAN DESIGN PROCESS OUTLINE

The design process is divided into seven stages. The first four stages define the site survey process and the last three stages describe the procedure for the LAN design and costing. In summary, the stages are as follows:

1. Select a design team and assess the LAN requirements, server needs, and remote access requirements.

2. Perform a preliminary site survey to collect communications closet data and survey existing equipment.

3. Analyze the preliminary site survey data, confirm communications closets, and define departmental region boundaries.

4. Complete the site survey to determine user and backbone cabling.

5. Develop the LAN design and describe four different performance variations.

6. Prepare a cost estimate for the new LAN and estimate the cost difference between performance variations.

7. Compare the four performance variations and select the final design.

EXAMPLE LAN DESIGN

LAN design example provided

To assist the reader, this guide presents an example of a LAN that is being designed for 141 Ethernet LAN users, nine remote LAN users, and a fiber distributed data interface (FDDI) backbone. The example includes site survey information and site survey checklist forms showing how this information is recorded. The example LAN design is found at the end of each of the seven stages.

Note: *To simplify the design process, any exceptions or special considerations are written in italics.*

LAN DESIGN FEATURES

Many standards and policies (as listed in appendix C), current networking practices, and engineering design choices have been incorporated into the design process. As a result, any LAN designed using this guide will incorporate the following features:

Ethernet and FDDI

Ethernet unshielded twisted-pair (UTP, also called 10BaseT), 10BaseF, and FDDI have been selected over all other existing standards-based communications protocols for each connection in the LANs. This choice was made to improve compatibility with future LAN designs or upgrades, increase network reliability and ease of installation and maintenance, and facilitate centralized management and monitoring. These communications protocols will be used for both user connections and building backbone connections. Where existing networks are connected to the new LAN, other communications protocols may be used, but must be converted with bridges, routers, or gateways to Ethernet or FDDI protocols.

Fiber Optic Inter-Repeater Link (FOIRL) is a de facto standard Ethernet interface, similar to 10BaseF. Many vendors supply equipment that supports both FOIRL and 10BaseF connections, and many people use the terms interchangeably. FOIRL interfaces can be used with equipment that supports both formats, with the understanding that equipment which is only FOIRL compatible may become insupportable in the future.

Star topology

To facilitate LAN user moves, adds, and changes and future equipment upgrades, the LAN will be laid out in a star topology with intelligent hubs at the center of each star. **If** more than one communications closet (sometimes called an intermediate distribution frame (IDF)) is needed, each closet will be connected to the building distribution frame (BDF) closet in a star topology. The BDF will provide connectivity to the post-wide backbone or other out-of-building cabling.

Design for maximum LAN user count

This design guide will help the user design a network with enough network user information drops, installed user cable, and departmental hub capacity to handle the maximum possible number of users in each area, not just the initial users. This design practice will ensure that as LAN users are added and moved there will always be an information drop for each LAN user, that additional hubs will not need to be added, and that new user cable will not have to be run several times during the life of the cable plant. The maximum number of LAN users will be estimated using the amount of floor area served by each communications closet or the number of information drops needed for each room, whichever is greater. The design uses one information drop per 40 square feet times 1.2 for sparing. See figure 3-1

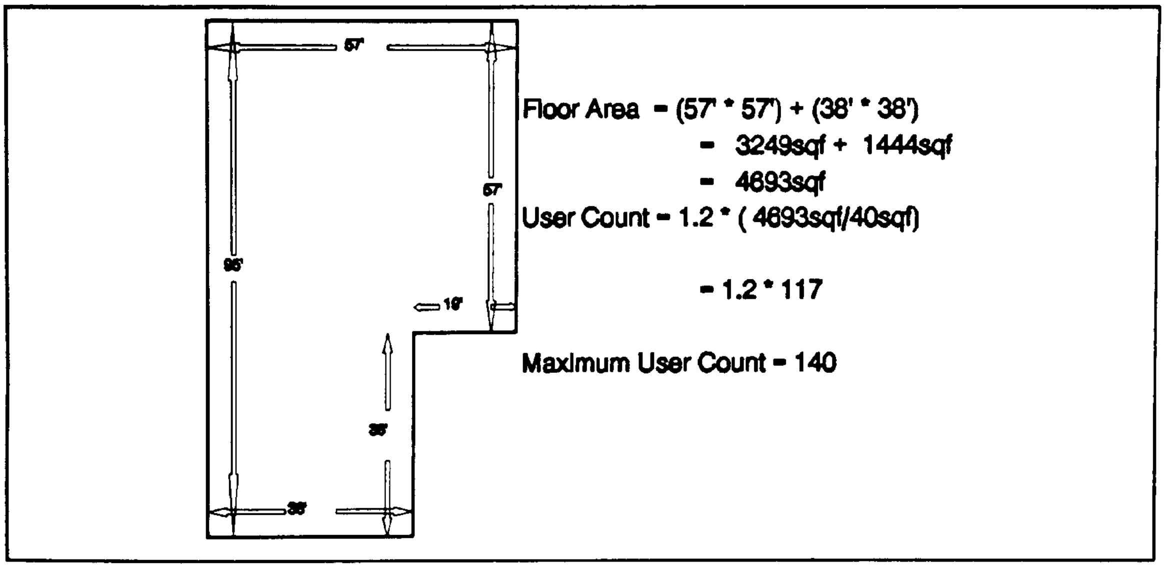


FIGURE 3-1. Maximum user count.

Unclassified network

To simplify the LAN design process and significantly reduce the equipment costs, LANs designed with this document will be used to carry only unclassified traffic and employ only normal, commercial network security procedures.

Rationale: Protection of Department of Defense (DOD) classified information is handled differently than network security issues. Design factors for National Security Agency (NSA) certification of a LAN are contained in:

- DoD 5200 series documents
- Director Central Intelligence Directive (DCID) 1/16-1, Security Manual for Uniform Protection of Intelligence Processed in Automated Information Systems and Networks
- Defense Intelligence Agency Manual (DIAM) 50-4, Security of Compartmented Computer Operations
- National Communications Security Information Memorandum (NACSIM) 5100A, Compromising

Emanations Laboratory Test Requirements, Electromagnetics

National Computer Security Center (NCSC)-TG-005, Trusted Network Interpretation.

These documents do not currently address certification of LANs beyond stand-alone isolated networks. The Orange Book is being rewritten to include multilevel security, installation/wide area connectivity, and Defense Message System architecture changes. Until that action is complete, all government secure LANs will be isolated systems operated at a system-high level.

Classified Systems: Until multilevel secure system requirements are defined and vendor equipment is designed and certified, the only way to create a network for handling classified data is to design a standard network and operate it in a secure area. Access to any portion of the system must be treated in the same way as access to any information on the system. Thus the network must be physically secured at a system high level equal to the highest level of classification of data accessible on the network.

Intelligent hub requirements

Intelligent hubs are used exclusively to provide ease of maintenance, centralized management, and future upgradeability. See figure 3-2 for a typical intelligent hub configuration. Each intelligent hub will have the following features.

Hub sizes

Intelligent hubs come in a wide range of sizes. To simplify the design process, intelligent hubs are described in two generic sizes: 6 slot and 12 slot. While these sizes vary between vendors, typically there will be 6 slots in the small hub and 12 slots in the full-sized hub. For networks with more than 10 hubs of either size, or networks servicing mission critical applications, it is recommended that one additional hub be purchased as a spare. Some slots will be occupied by Ethernet Simple Network Management

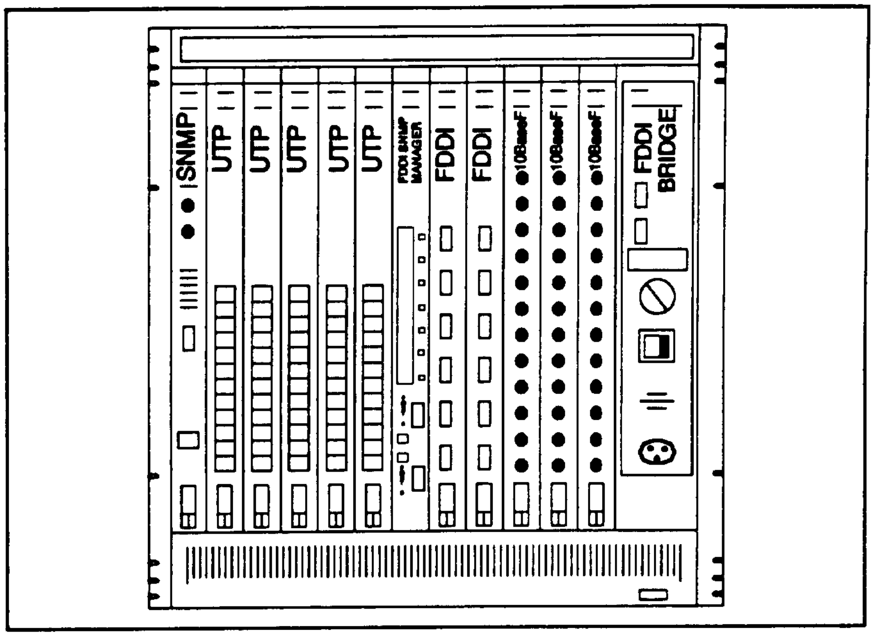


FIGURE 3-2. Typical intelligent hub configuration.

Protocol (SNMP) management modules, Ethernet retiming modules, FDDI SNMP management modules, FDDI backbone connection modules, power supply modules, and bridging modules. The number of slots remaining for user input/output (I/O) modules is reduced by these essential modules, and varies from vendor to vendor. The hub I/O module capacity as used in the stage 5 design process and as found in the Certified Components List (CCL) refers to the number of I/O modules that can be placed in a fully configured hub, not the total number of slots in an empty chassis.

Power supplies

The hubs will use load sharing, hot-swappable power supply modules to allow maintenance or repair with minimal disruption of the network. A minimum of one additional power supply module, to be used as a spare and to facilitate repairs and maintenance, is recommended. For large networks, this should be increased to one spare power supply module for each 20 hubs.

SNMP management

Each hub will have full SNMP compatible management of all Ethernet connections and FDDI connections, if used. This will facilitate centralized network management and monitoring of network performance. A minimum of one additional SNMP management module, to be used as a spare and to facilitate repairs and maintenance, is recommended. For large networks, this should be increased to one spare SNMP management module for each 20 hubs.

FDDI attachment and management

Each hub that supports FDDI user connections may require additional station management (SMT) module to manage all FDDI connections and provide an FDDI backbone to hub backplane connection. This will facilitate centralized network management, monitoring of network performance, graceful inserts and removes, and validation and control of FDDI connections. To ensure optimal network operation, the FDDI attachment and management must support a primary, secondary, and local loop; connection validation; and graceful inserts and removes. To accomplish these goals, the FDDI attachment and management must have a minimum of two media access control (MAC) units. A minimum of one additional FDDI attachment and management module, to be used as a spare and to facilitate repairs and maintenance, is recommended. For large networks, this should be increased to one spare FDDI attachment and management module for each 20 hubs supporting FDDI connections.

Local bridge

Each departmental communications closet hub will include a local bridge, either Ethernet-to-Ethernet with a 10BaseF connection or FDDI-to-Ethernet with an FDDI connection. The local bridges will help to limit network congestion in multihub LANs. A minimum of one additional local bridge, to be used as a spare and to facilitate repairs and maintenance, is recommended. For large networks, this should be increased to one spare local bridge for each 20 hubs.

Where possible, this bridge will be an internal module, but some hub vendors may require either an external bridge or an external media conversion transceiver. This will affect the amount of rack space needed by each hub for some LAN designs. Optionally, some or all of the local bridges might be located in the BDF closet and combined in the form of a multiport bridging hub or multiple Ethernet ports in a router.

I/O modules

Each intelligent hub will support I/O modules for Ethernet 10BaseT (UTP) and 10BaseF connections and for FDDI user connections. The FDDI modules must allow users to be added or removed during network operation without disrupting the FDDI ring or other users on the FDDI ring. This must include unexpected power-off/power-on events as well as scheduled insertions and removals. Other interface protocol modules can be used to connect to existing networks. A minimum of one additional I/O module of each type used in the network is recommended as a spare. For large networks, this should be increased to one spare I/O module of each type for each 20 modules.

User cable requirements

To comply with the Installation Information Transfer System (IITS) Policy to improve long-term reliability and to provide for future upgrades, a hybrid cable will be used for the run from the communications closet to each user information drop. This hybrid cable will consist of eight twisted wire pairs, to support both network and Integrated Services Digital Network (ISDN)/telephone company (telco) connections, and four strands of fiber optic cable, to support 10BaseF or FDDI single- or dual- attach. See figure 3-3.

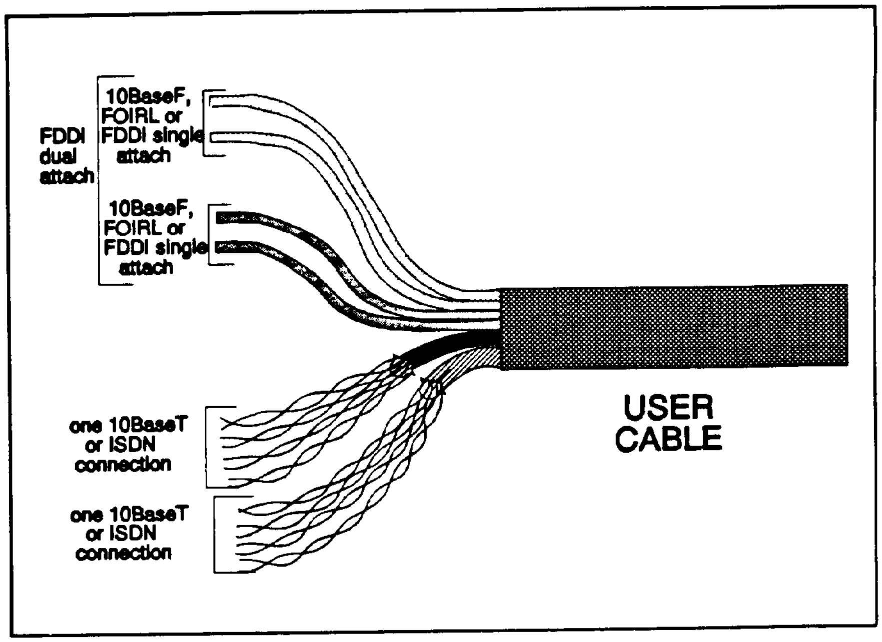


FIGURE 3-3. User cable.

The eight UTP will comply with category 5 attenuation and noise immunity standards. Each fiber optic strand will consist of multimode fiber, with a core diameter of 62.5 microns and a cladding diameter of 125 microns. Each fiber should be rated at two different wavelengths of light, at 850 nanometers (nm) for 10BaseF and at 1300 nm for FDDI. The fibers should have a maximum attenuation of 3.75 decibels (dB) per kilometer at 850 nm and 1.0 dB per kilometer at 1300 nm, and a minimum bandwidth of 160 megahertz (MHz) per kilometer at 850 nm and 500 MHz at 1300 nm. Plenum rated cable should be considered if the user cable runs will include raised-floors or drop-ceilings that contribute to office air flow.

To prevent expensive incremental additions to the cable plant, a separate user cable will be installed for each user information drop location. The cable will be terminated at patch panels in the communications closet and wall plate units in the office/work area. See figure 3-4. All unused wires and fibers will be terminated and reserved for future upgrades. When purchasing user cable, an additional 20 percent will be added to ensure sufficient cable for installation and maintenance.

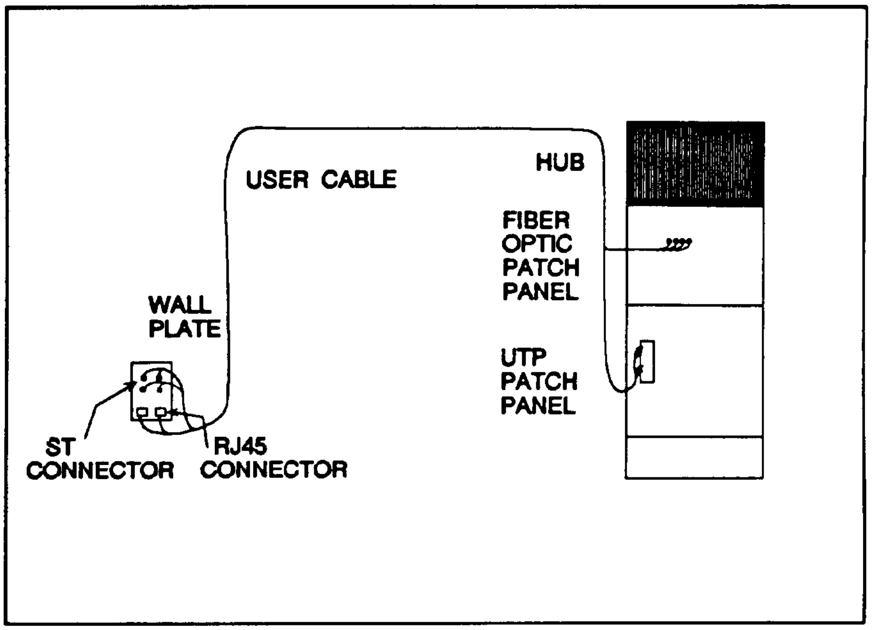


FIGURE 3-4. Composite cable terminations.

Building backbone cable requirements

To support long cable runs between communications closets and high-speed backbone communications, a 12-strand 62.5/125 multimode fiber optic cable will be used for all connections between communications closets. This fiber will support either Ethernet 10BaseF or FDDI connections. For FDDI dual-attach connections between communications closets, this will leave eight dark fibers to handle additional capacity or new connections. Use of fiber optic cable instead of UTP or coax between communications closets will support backbone bandwidth upgrades, greater distances between communications closets, and migration to new technologies.

Each fiber should have a maximum attenuation of 3.75 dB per kilometer at 850 nm and 1.0 dB per kilometer at 1300 nm, and a minimum bandwidth of 160 MHz per kilometer at 850 nm and 500 MHz at 1300 nm. Since some of these cables may be run in vertical plenums between floors in a building, or horizontally in raised floor or drop ceiling air plenums, all backbone cables will be plenum rated (Fire Code Safety Regulations).

A fiber optic cable will be run from each intelligent hub in each communications closet to the BDF closet. The unused fibers in each cable will allow for easy upgrades, such as adding more hubs, segmenting existing hubs, and implementing new technology for the building backbone. Each backbone cable will have all fibers terminated on patch panels at both ends. When purchasing backbone cable, an additional 20 percent will be added to ensure sufficient cable for installation.

Patch Panels

To prevent damage to installed cables, tangling of cable bundles, and loss of installed cable labels, the communications closet end of the user cables and both ends of the backbone cables will be terminated in patch panels, not run directly into hub modules. For similar reasons, the user end of each user cable will be terminated in a wall or floor plate, with RJ-45 connectors for each 4-pair UTP cable and snap-twist (ST) connectors for each fiber optic strand.

Patch cables will be used in each closet for patch panel-to-hub module connection. Ten meter cables will be used to connect each user's computer to a wall/floor plate. The patch cables will then take the stress and wear of moves/adds/deletes, module swaps, and other communications closet activities that might otherwise damage LAN building cabling and terminations.

The UTP patch panel can either be implemented with RJ-45 connectors or 110-A punch down blocks. RJ-45 based patch panels are recommended for new buildings, and 110-A punch down blocks are recommended for upgrades in old buildings. All UTP patch panels, patch cables, hookup wire, and wiring practices must maintain category 5 attenuation and noise immunity standards. This will allow migration to 100 megabits per second (Mbps) over UTP communications technologies in the future and will assure reliable operation for standard Ethernet or ISDN.

Fiber optic patch panels and wall/floor plate connectors will use ST connectors. This is an industry standard connector, with good operating characteristics. The industry has developed equipment and procedures for field termination of these connectors. The fiber optic patch panels must be rack mounted or physically secured if racks are not available. The fiber cables or fiber strands from the composite cable must be routed, bundled, and secured to prevent flexing, stretching, or breaking.

Existing LANs

This LAN design process assumes that a new LAN is being designed. For sites with existing network servers and user workstations, this equipment will be included in the new network.

Since the cost of researching and documenting existing equipment and cabling, adapting non-standards-based equipment, and engineering a custom integration plan is often more expensive than the equipment saved, it may be better to start fresh with all new equipment. For this reason, existing network infra-structure equipment, such as fan-out boxes, thin or thick coax, or repeaters, will not be incorporated in the LAN design in this document.

Bridges in building, routers out of building

In this LAN design, bridges will be used for all network segmentation within a building, and routers will be used for connecting the building backbone to a post-wide backbone. Each departmental communications closet will connect to the BDF closet with a bridge, and the BDF will connect to the post-wide backbone with a router. The only exception is if a multiport bridge is used in the BDF. In that case, an external router is used to connect to one of the bridge ports or a multiport router is used.

The reason for using bridges inside the building is that they are usually cheaper and faster than routers. Bridges provide a cost effective degree of isolation for a small network, and simplify monitoring network activities from a single location. Bridges work well in a star topology, and there is usually little need for different internet protocol (IP) network addresses within a building.

Routers are recommended for the out-of-building connection because a greater degree of isolation is desired at this point, and the post-wide network is larger and more complex. Routers will protect the post-wide backbone against broadcast storms, provide IP network segmentation, and provide greater security and packet filtering for each building.

LAN DESIGN VARIATIONS

To provide a trade-off between network performance and equipment cost, the basic design is developed with four different performance variations in stages 5, 6, and 7 of the design process. These four performance variations consist of a basic Ethernet design and three enhancements to the basic design. Each variation differs only in the technique of building backbone connection and the choice of Ethernet or FDDI user connections.

Basic Ethernet/ Ethernet

This variation provides Ethernet (10BaseT and 10BaseF) to the LAN user and an Ethernet (10BaseF) building backbone (between communications closets). This design variation provides the lowest level of network performance of the four variations and is considered to be the baseline cost. Figure 3-5 shows a possible network configuration with intelligent hubs containing 10BaseT and 10BaseF modules.

The local bridges can either be internal modules in each hub or external devices, as shown in the figure 3-5. The backbone cable shown in the figure is multimode fiber and the user cable is a UTP/fiber optic composite cable. The router and connection to a post-wide backbone are optional and are not part of the LAN design process.

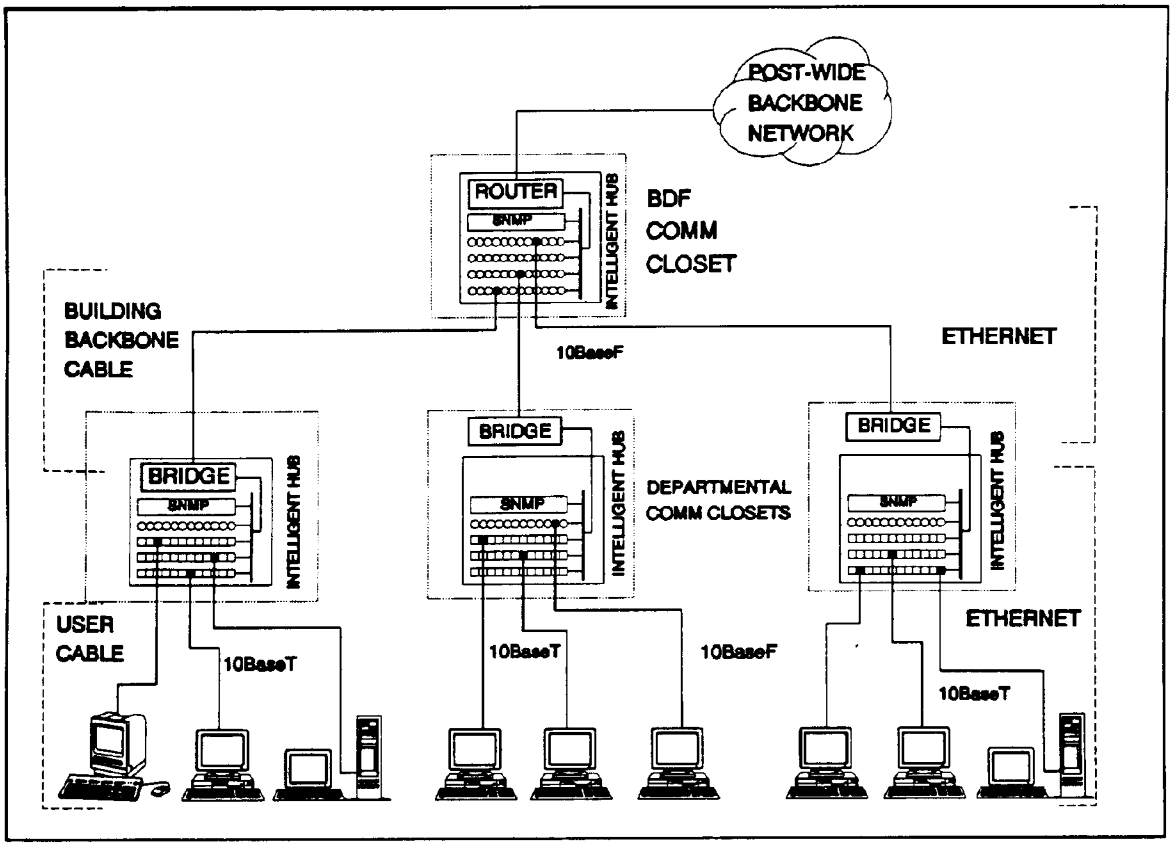


FIGURE 3-5. Basic Ethernet/Ethernet network configuration.

Multiport Ethernet/Ethernet

This variation provides Ethernet (10BaseT and 10BaseF) to the LAN user and an Ethernet (10BaseF) building backbone (between communications closets). The backbone uses a multiport bridge to enhance performance. This variation provides greater performance than the basic design and at potentially less cost than the basic design. Figure 3-6 shows a possible network configuration that is the same as figure 3-5, with the exception that the BDF intelligent hub has been replaced by a multiport bridging or routing device. The local bridges in each communications closet have been removed, since the BDF bridge already performs the same functions. The connection to a post-wide backbone is optional.

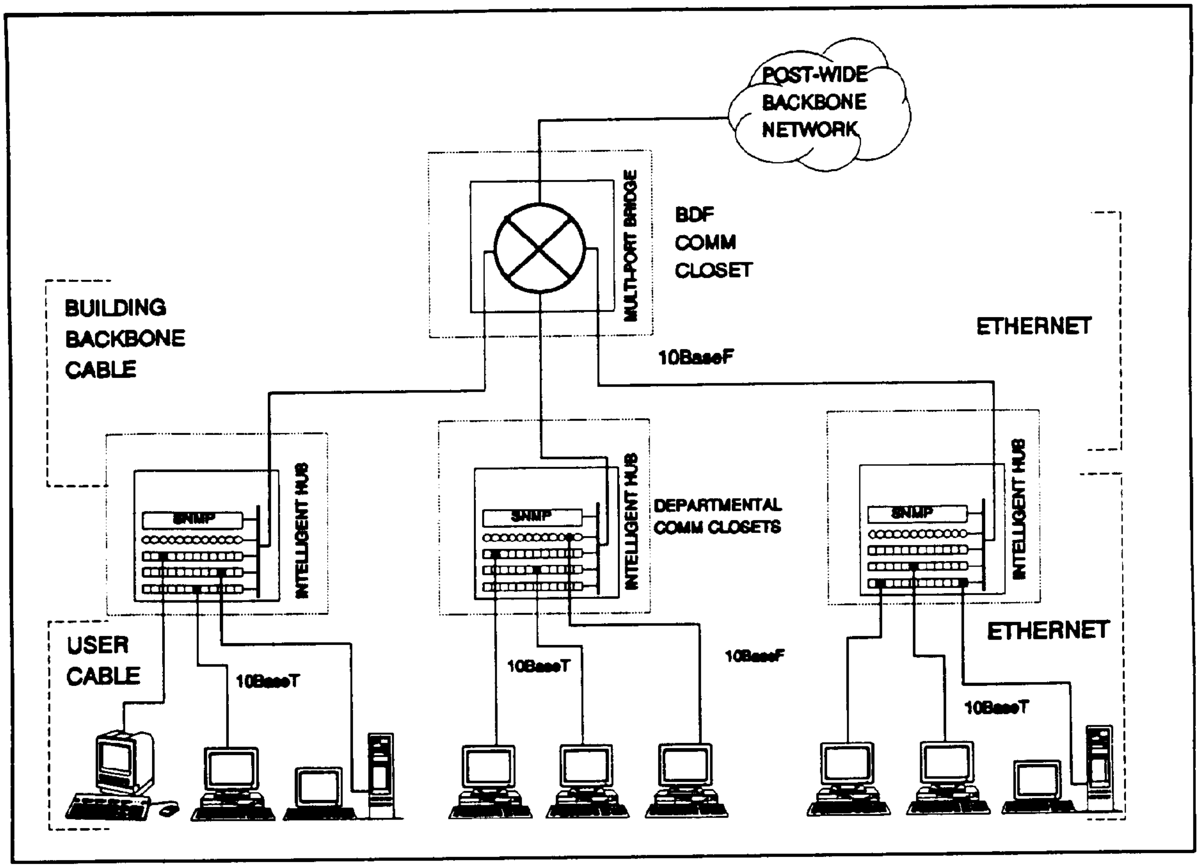


FIGURE 3-6. Multi-port Ethernet/Ethernet network configuration.

Ethernet/FDDI

This variation provides Ethernet (10BaseT and 10BaseF) to the LAN user and an FDDI building backbone. This design will provide higher performance and more long-term growth potential, but at a somewhat higher cost than the Ethernet backbone variations. Figure 3-7 shows a possible network configuration, similar to figure 3-5, except that the 10BaseF based Ethernet backbone has been replaced with an FDDI backbone, using the same backbone cable. The local bridges in each communications closet translate FDDI to Ethernet, as well as filter local traffic. The FDDI loops shown in the figure could represent either single fibers providing single-attach master-port (M-port) to slave-port (S-port) connections, or two fibers, each showing dual-counter-rotating (A and B port connections) or dual-homed connections. The router and connection to a post-wide backbone are optional.

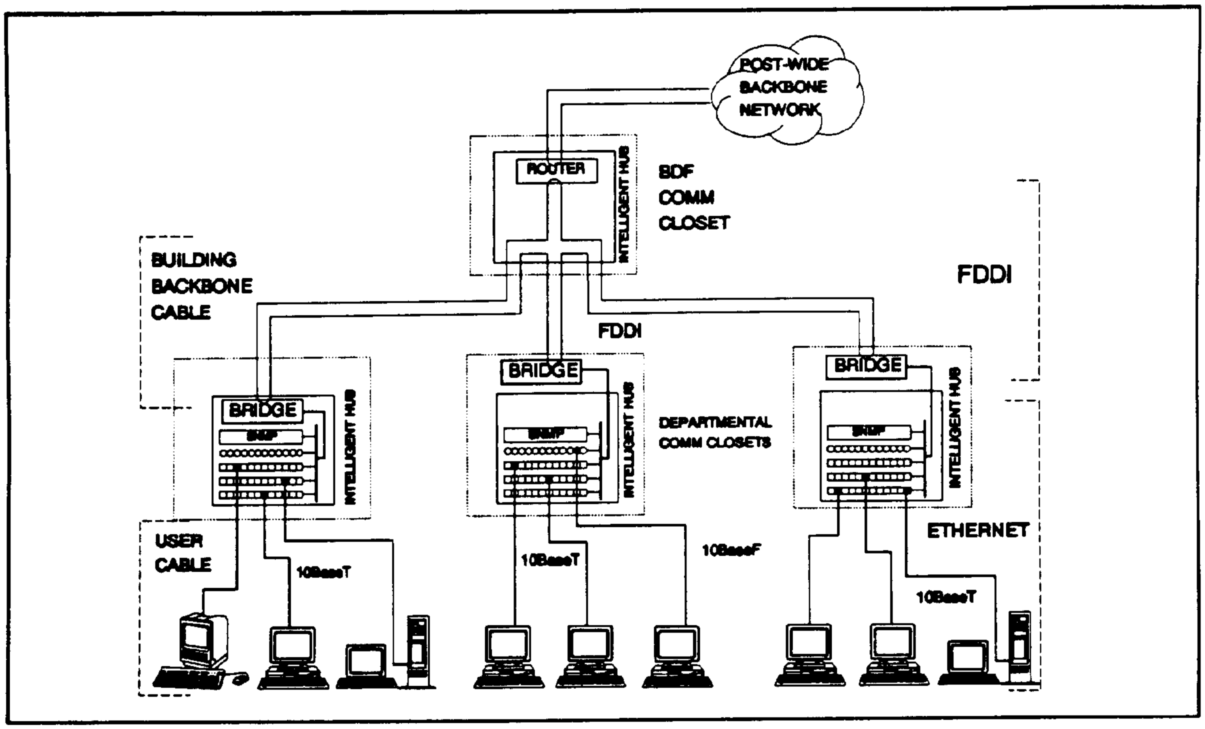


FIGURE 3-7. Ethernet/FDDI network configuration.

Hybrid/FDDI

This variation provides both Ethernet (10BaseT and 10BaseF) and FDDI to the LAN user with an FDDI building backbone. This design will provide the highest performance, with good long-term growth potential, but at a higher installation cost. The term "hybrid" refers to the fact that both Ethernet and FDDI are used for LAN user connections. Figure 3-8 shows a possible network configuration with two of the communications closets providing FDDI connections to user workstations. The FDDI connections between the intelligent hubs and user workstations are shown in an idealized form in figure 3-8. In an actual installation, the hub would contain FDDI interface modules and an FDDI management or system attachment module. The router and connection to a post-wide backbone are optional.

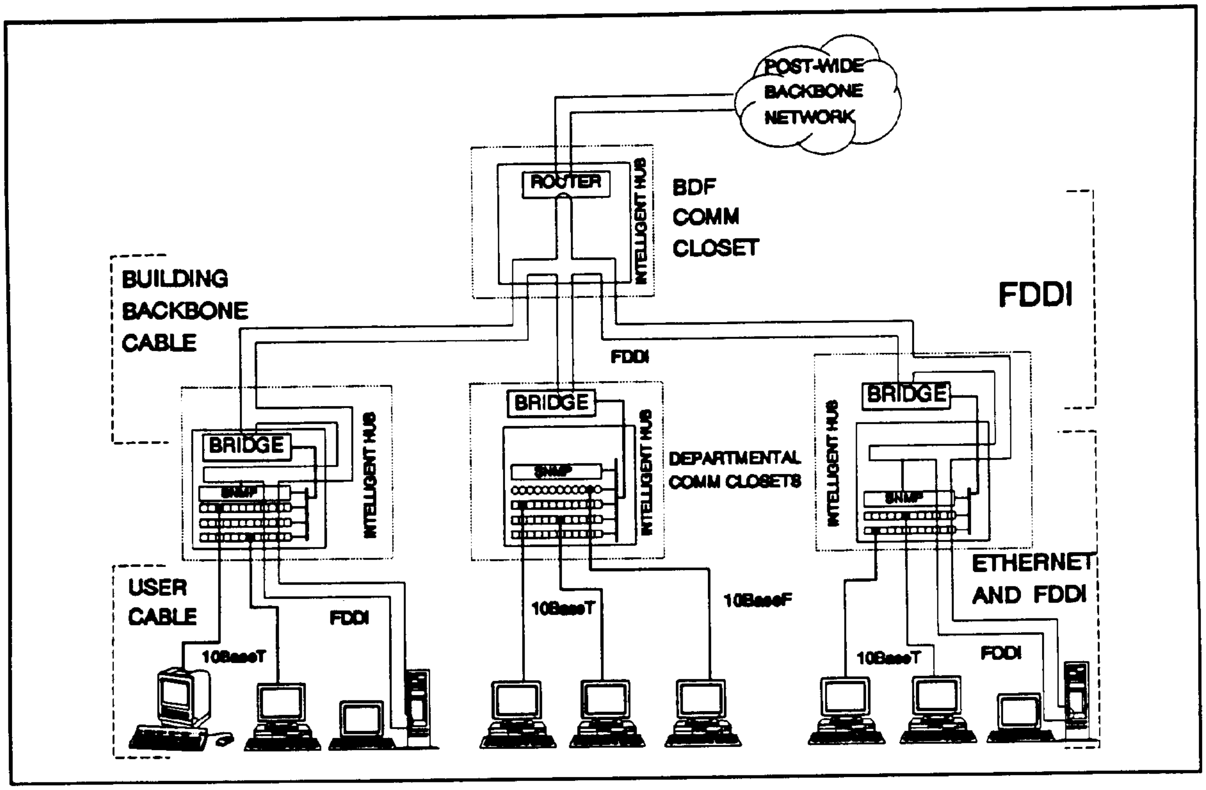


FIGURE 3-8. Hybrid/FDDI network configuration.

STAGE 1 - LAN NEEDS ASSESSMENT

GENERAL

During the LAN needs assessment stage, the members of the LAN design team are selected, site survey forms are prepared, and the LAN requestor is interviewed to define the requirements of the new LAN. The information from the LAN requester is recorded in the Site Survey Checklist Checklist 1A. Blank copies of the Site Survey Checklist can be found in appendix B of this document, and should be copied as needed.

SELECT LAN DESIGN TEAM

The Director of Information Management (DOIM) will select a LAN design team. The members and responsibilities of the LAN design team must be decided before the LAN design process can begin. The design team must include a site survey team, people to analyze the site survey data, people to do the actual network design, and people to authorize vendor selections and cost performance trade-off decisions. The site survey team should include LAN technicians and cable installers with experience in user workstation setup/maintenance, server setup/maintenance, network hubs, bridges, repeaters, and inside plant cabling. The design team should also include people with systems analysis/network design engineering experience. These individuals should be responsible for directing the design team, directing the site survey team, approving vendor selections, and approving cost performance trade-off decisions.

PREPARE FLOOR PLANS

Use D-sized engineering floor plans when possible. These drawings can usually be requested from the Facilities Engineer or the Director, Engineering and Housing. Engineering drawings should be requested as far in advance as possible. Add any cable runs, cable trays, ducts, or cable conduits that are not on the drawings. Make three copies of the floor plans for each area covered by the LAN. Label each floor plan with the project name, post name, building, floor or area, and date. Also mark each floor plan to show that it is being used for the LAN design process. Label the copies: 1) SITE SURVEY; 2) COMMUNICATIONS

CLOSETS; and 3) USER DROP LOCATIONS.

If D-sized engineering drawings are not available, smaller scaled drawings may be used. To improve readability of the floor plans, the largest size available should be used. Drawings not to scale should be avoided if at all possible, since cable run lengths will not be accurate. If new drawings are created, U.S. Army Information Systems Engineering Command (USAISEC) Regulation 34-3 and USAISEC Pamphlet 34-3 should be followed.

PREPARE SITE SURVEY CHECKLIST 1A

Make a copy of Checklist 1A (LAN Needs Assessment), found in appendix B at the back of this document. Fill in the Site Survey location data in lines 1-A through 1-G to identify which LAN design project this Checklist is for, and to identify the points of contact.

INTERVIEW LAN REQUESTOR

Check with the LAN requestor to see if an information capability request (CAPR) or special funding has been approved for the new LAN. Record the **CAPR or funding for project approved (Checklist 1A, line 2).** The CAPR should contain information on the LAN size, purpose, and requirements. Obtain the estimated LAN user count from the LAN requestor. Include both current and planned LAN users in the LAN user count. Record the **Estimated LAN User Count (Checklist 1A, line 3).**

Out-of-building connection

Determine if a connection(s) is needed to other buildings and enter **Connection to LAN's In other buildings (Checklist 1A, line 4-A).** If a connection is needed to the Defense Information Systems Network (DISN) or to the post-wide backbone (Common User Installation Transport Network (CUITN)), record the information on Checklist 1A, lines 4-B and 4-C.

Existing servers

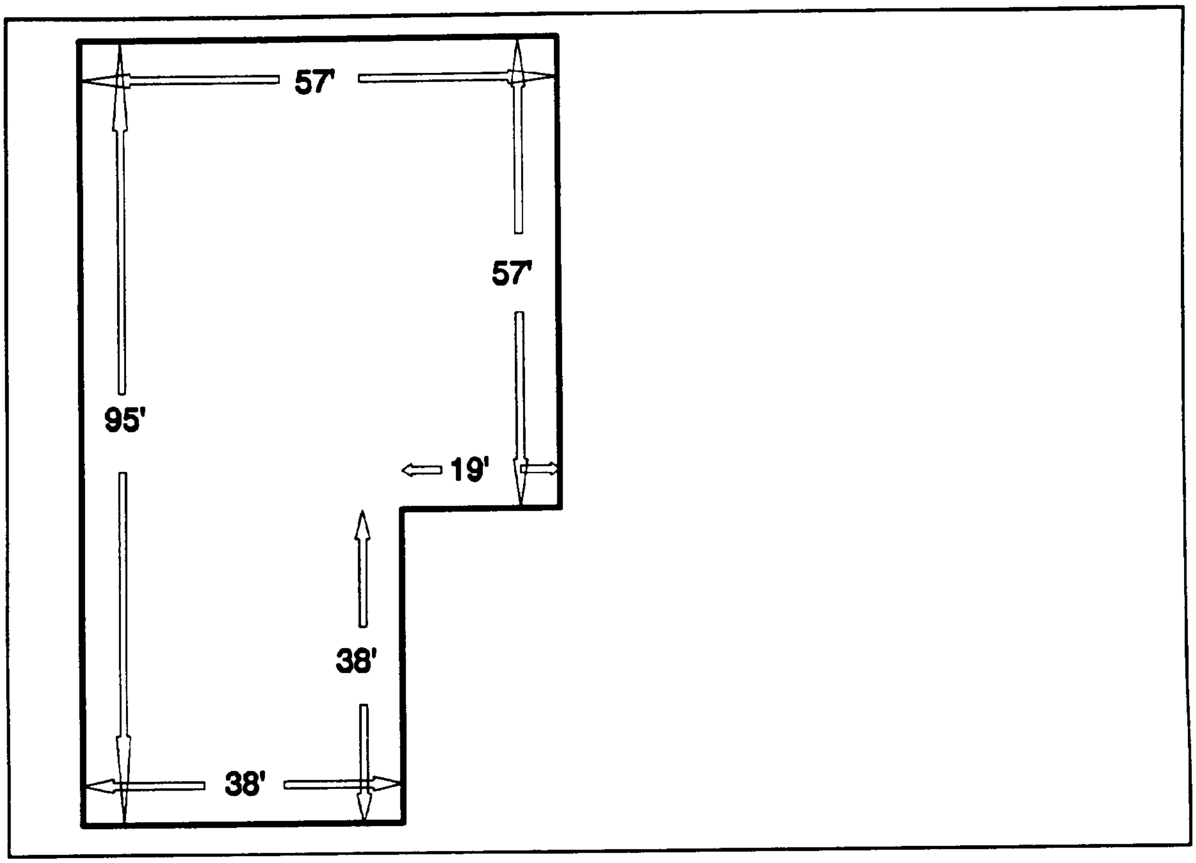
Interview the LAN requestor for information about any existing servers that may be compatible with the new network. Record information for existing servers on Checklist 1B.

EXAMPLE LAN DESIGN

The DOIM has received a request for a LAN to be installed on the first floor, Building 1001, Fort Redrock. The DOIM selects a design team. The design team prepares a site survey. A copy is made of the Site Survey Checklist 1A, from the blank forms in appendix B. In line 1-A, the team gives this project the name "Example LAN Design." In line 1-B, the name of the post, Fort Redrock, is entered. In line 1-C, the building number of 1001 is entered. Since the new LAN will only be installed on the first floor of this one building, line 1-D is "First Floor." The survey date of 30 September, 1993 is entered in line 1-E. The name of the LAN requestor, SFC Brown, is entered in line 1-F, along with his telephone number (555-1234). Since the DOIM is supervising this LAN design effort, his name and number are entered in line 1-G. To avoid confusing the Example LAN design Checklists with checklists from any other project in progress, the project name, Example LAN Design, is put on most of the Site Survey Checklists.

The team acquires copies of the present floor plans, as shown in example figure 1. The team interviews LAN requestor SFC Brown. In line 2 of Checklist 1A, the team records that the CAPR for a new LAN has been approved, and that a tentative spending limit of $200,000 has been set. SFC Brown indicates that he currently knows of about 35 users in the building that need LAN connections and 9 computers in trailers temporarily assigned to his building that will initially need LAN connections. The survey team then enters an estimated user count of 45 in line 3. It should be noted that the LAN design will be sized on the floor space, not this estimated user count. This estimate, however, will be used to confirm that the LAN design is big enough, and that the design has not grown too large. Using Checklist 1A, lines 4-A through 4-C, the team records that SFC Brown indicates there are no requirements for out-of-building connections. Example figure 2 shows a completed Checklist 1A. Checklist 1B is not used because SFC Brown knows of no existing servers.

After the interview, the team labels and identifies the floor plans, to include modifications and changes.



EXAMPLE FIGURE 1. Blank floor plan.

SITE SURVEY CHECKLIST 1A
LAN NEEDS ASSESSMENT

1. Survey Location Data
   - A. Name or number of LAN design project : *Example LAN Design*
   - B. Name of post : *Fort Redrock*
   - C. Name or number of building(s) : *1001*
   - D. Name or number of floor(s) : *First Floor*
   - E. Date survey performed : *09/30/93*
   - F. Name of LAN requestor : *SFC Brown*

     Telephone number : *555-1234*
   - G. Name of person performing survey : *DOIM*

     Telephone number : *555-1000*
2. CAPR or funding for project approved : *CAPR approved, funding limit of $200,000*
3. Estimated LAN user count : *45*
4. Out-of-Building Connection
   - A. Connection to LAN's in other buildings (Yes/No) : *NO*

     List :

     other :

     buildings :

     :
   - B. Connection to the DISN gateway (Yes/No) : *NO*

     Location of DISN gateway :
   - C. Connection to post-wide backbone (Yes/No) : *NO*

     CUITN connection already in the building (Yes/No) :

     Location of nearest CUITN attach point :

EXAMPLE FIGURE 2. Stage 1 Checklist 1A.

STAGE 2 - PRELIMINARY SITE SURVEY

GENERAL

During the preliminary site survey, the survey team will prepare copies of site survey checklists needed in Stage 2, collect communications closet data, and survey existing network equipment, servers, user workstations, and applications software usage. The survey team will collect information on the communications closets' physical and electrical suitability. Information on initial LAN user locations, applications used, and departments or work groups will be collected to help define departmental boundaries for each communications closet. The survey team will use the first copy of the floor plans (labeled "SITE SURVEY") and copies of Site Survey Checklists 2 and 3.

PREPARE STAGE 2 SITE SURVEY CHECKLISTS 2, 3

Make a copy of Checklist 2A, Project Data; copies of Checklist 2B for each building in the project; and copies of Checklist 2C for each floor in the project. Make a copy of Checklist 3 for each communications closet and potential location for a communications closet.

COLLECT COMMUNICATION CLOSET DATA

Survey the building(s) to be covered by the new LAN. Collect data on all possible communications closet locations and their physical and electrical suitability.

To avoid repeating pan of the preliminary site survey, be sure to include even potential locations in all areas. As a rule of thumb, include at least one current or possible communications closet location in each 10,000 square foot area.

Existing communications closet locations

List <u>all building numbers to be served by this LAN project (Checklist 2A, line 2)</u>. For each building on Checklist 2A, complete a copy of Checklist 2B listing each floor that will be served by this project. Use copies of Checklist 2C to identify the communications closets on each floor. Mark and label the location of each communications closet on the SITE SURVEY copy of the floor plans.

Check with the DOIM, the facilities engineer, and telephone equipment personnel to see if a labeling convention for each closet already exists. Determine whether new equipment or changes are expected in any of the closets identified. If no current closet labels exist, a possible labeling convention is to concatenate a hub number, floor letter, and building number. For example, 3A1001 would be the third communications closet on the first floor of building 1001. If this design is only for a single building, this can be simplified to just a letter and number. You can also use names like planning, accounting, Standard Installation\Division Personnel System (SIDPERS), etc., for closets that will have specific LAN users. Enter **the closet label and location Information (Checklist 3, lines 2 through 3-F).**

New or possible communications closet locations

In some areas to be covered by the LAN, there might not be an existing communications closet within a 10,000 square foot area, or the communications closet might not have enough room for the hubs and servers, or it might be unsuitable for other reasons. In these cases, it may be necessary to identify new closets or convert existing rooms into communications closets. New communications closet construction, or major modification of existing locations, should be defined in the Site Concurrence Memorandum described in section 4, part 2, of this document. In general, the LAN hardware should only be combined with telephone company (telco) equipment or placed in a computer room.

Once a possible new communications closet location has been found, mark it on the floor plan and label it like an existing communications closet.

Identify BDF closet

While surveying communications closet locations, look for a communications closet to use as the center of the building backbone. This will typically be the same location used as the telco central connection. When identifying a BDF closet, consider the backbone cable runs to other closets, which will have a 3000 foot limit for 10BaseF/FOIRL connections. Also consider that if user connections will be supported in the same closet, there must be room for user hub(s) and backbone hub(s). One hub can only be used if the internal backplanes can be segmented, and the users can be separated from the building backbone. To provide this separation, a local bridge must be used between the user connections and the backbone connections, even if they are in the same hub. For simplicity and ease of maintenance and future expansion, it is highly recommended that separate hubs and patch panels be used for the user connections and the backbone connections. The BDF should also have a lockable door to prevent accidental damage or tampering. The BDF should also contain a UPS to prevent disruption of the building backbone or out-of-building connections during a power failure. The BDF is also a good location for network servers, if there is enough room. Identify the communications closet as "BDF" in **(Checklist 2C, line 2-C and Checklist 3, line 2).**

Racki cabinet space

Exisung unused rack space, and potential rack space if new racks are installed, must be measured to determine how much LAN equipment can be installed. For this survey, rack space is measured in two categories:

1) Currently installed racks with unused space into which LAN equipment can be mounted.

2) Empty floor space where new racks can be installed.

If racks are currently installed, check to see if there is any unused space in the cabinet. Check behind any blank panels for empty space. Do not consider slots less than 3.5 inches in height. Measure the unused space in terms of height. Record the **Unused rack/cabinet space (Checklists 3, line 4-A)** in inches.

If any of the potential LAN closet locations have other equipment already installed, check with the responsible activities tor the equipment to make sure that currently unused space can be used for LAN equipment. Addition of new equipment, cables, or racks must be coordinated with all LAN users of the closet.

If there is any empty floor space, measure it to determine whether it is at least 24 inches wide and 40 inches deep.

For safety, there should be 30 inches clearance for people installing or maintaining the equipment. If there is sufficient space for more racks, measure the space vertically to determine the tallest rack that can be installed. Record the total amount of **Potential rack(cabinet space (Checklist 3, line 4-B)** in inches.

Ac power availability

It is strongly recommended that a new or dedicated 20 amp BLACK filtered alternating current (ac) power circuit be available for each LAN hub. The circuit should have no other loads connected to it to provide clean reliable power. Servers should also have BLACK filtered ac power. A uninterruptible power supply (UPS) is recommended for each server. Check with the facility engineer to find the number of ac power circuits available in the communications closet with adequate "ampacity" and no other loads. Record the **Number of unused 20 amp power circuits available for LAN use (Checklist 3, line 4-C).**

Heating, ventilation and air conditioning (HVAC)

LAN equipment is sensitive to overheating, temperature extremes, and rapid temperature variations. Each communications closet should have a ventilating duct or vent panels in the door. If the communications closet requires additional ventilation, identify **Additional ventilation required (Checklist 3, line 4-D).**

Communications closet cable routing capacity

Check that the cable trays, cable conduits, and openings entering the communications closet have enough unused space to handle the additional cables required for the new LAN. As a rule of thumb, use a 4-inch thick bundle for each 100 cables. Estimate the **Floor. Ceiling. Walls Cable routing capacity (estimated number of additional cables) (Checklist 3, line 4-E).** Also note if there are any obstructions that will interfere with running the cables to current or added racks. (Signal and power cables will not be run together.)

User cable routing considerations

To assist in defining the departmental regions for each communications closet, it is necessary to determine if there are any cable routing barriers between the communications closet and the user information drop locations. Record on the site survey floor plans any impediments to cabling, such as fire walls, small hallways with no raised floors or dropped ceilings, and distant wings or annexes. Also, mark the floor plans to show areas with raised floors or drop ceilings. If necessary, create a fourth copy of the floor plans to show clearly the raised floor, drop ceilings, cable runs, and cable barriers.

In some cases, it may be more cost effective to separate one region into two, in order to avoid running more than one cable across a hallway or other barrier that may require extensive modification for cable routing.

Physical security

The LAN equipment, and any servers not kept in user areas, should be protected by a lockable door or cabinet. Record whether or not there is a **Lockable door to Communications Closet or lockable electronics Cabinet (Checklist 3, line 4-F)**. If the closet has a lockable door, check the key control policies for that door to make sure that the LAN staff will be able to access the equipment and the equipment will be adequately protected from casual intrusion.

This concludes the initial communications closet table entries. The remainder of each Checklist 3 will be completed in later stages of the design process.

SURVEY EXISTING EQUIPMENT

Existing network infra-structure equipment, servers, and user workstations must be located, identified, and recorded on the site survey floor plans. The existing equipment records will document the existing configuration, identify equipment that can be used in the new LAN, and help define the cut-over plan and test procedures. If there is no existing networking equipment, continue to search for computers that can be used as servers or user workstations.

Existing network infra-structure equipment

Record on the site survey floor plans the locations and descriptions of the existing network infra-structure equipment and cabling such as thick coax, thin coax, attachment unit interface (AUI) cables, fan-out boxes, work group concentrators, and repeaters.

For existing equipment other than cabling, create copies of Form IC for each item, including spares. Record the project name in **Name or number of new LAN design project (Checklist 1C, line 1).** For each existing network, record the **Name of existing LAN or organization supported by existing LAN (Checklist 1C, line 2-A),** or the function that it performs. Record the physical interface(s) used in the LAN, such as Token Ring, T1 or fractional T1, or Ethernet and type(s) of cable used, such as UTP, thicknet, thinnet, or fiber on **Existing LAN type (Checklist 1C, line 2-B)**. For existing workstations and servers, record the **Number of workstations connected to existing LAN (Checklist 1C, line 2-C)** and the **Number and type(s) of servers connected to existing LAN (Checklist 1C, line 2-D)**. For any workstation to be transferred to the new LAN, ensure that a copy of Checklist 4-A is filled out. For each server that will be transferred to the new LAN, ensure that a copy of Checklist 1B is filled out. Record any use of existing equipment in the new LAN in **Will existing servers or workstations be transferred to new LAN (Checklist 1C, line 2-E)**.

Identify the item of equipment and its major function (hub, fan-out box, bridge, repeater, etc) and provide a description (rack mount/table top, number of ports, type of interface on each port, etc.) on **Type of equipment (Checklist 1C, line 3-A)**. Enter the item's **Manufacturers name (Checklist 1C, line 3-B), Product name (Checklist 1C, line 3-C), Model number (Checklist 1C, line 3-D),** and **Serial number (Checklist 1C, line 3-E).** Record the current configuration, modules or interfaces installed, software and revision if known, any modifications or additions not normally included, etc in **Configuration/options. number and type of ports (Checklist 1C, line 3-F).** Record the current location on **Name or number of building equipment currently installed in (Checklist 1C, line 3-G), Name or number of floor equipment installed in (Checklist 1C, line 3-H)**, and

Approximate location within floor of equipment (Checklist 1C, line 3-I). The current location should also be marked on the floor plans and labeled so that the equipment forms can be matched up to the floor plan locations. If possible, determine which software protocols can be used on this equipment, and list them on **Software protocols supported (Checklist 1C, line 3-J)**. Check to see if the equipment will support transmission protocol-4/connectionless network layer protocol (TP4/CNLP), transmission control protocol (TCP)/IP, and SNMP management to determine whether or not it might be compatible with the new network. Record SNMP support on **Does equipment support SNMP management (Checklist 1C, line 3-K)**, and TP4/CNLP or TCP/IP support on **Is equipment compatible with and available for use with new LAN (Checklist 1C, line 3-L)**.

Because of the cost of verifying cable routes, confirming patch panel and connector pin-outs, testing cable plant quality, engineering custom equipment integrations, verifying equipment interoperability, and assuring centralized network management and future upgradeability, the existing equipment cannot be economically used in the new LAN, and is not be covered in the LAN design.

Existing Servers

For each existing server or existing computer that will be used as a server in the new LAN, record the current location on the site survey floor plans. Use a copy of Checklist IB for each existing server or required server and document its current configuration. Servers should in general be considered for FDDI connection.

Existing user workstations

For each existing user workstation, record the current location on the site survey floor plans. The workstation locations will be used for refining communications closet boundaries and determining initial I/O module needs in each communications closet. Use a copy of Checklist 4A for each workstation to document its current configuration. Record the workstation's **User name and location (Checklist 4A, line 2)**. Identify for each workstation the **Network services needed (Checklist 4A, line 3)**. For each workstation, record the **Workstation type (Checklist 4A, line 4)**, the **Operating system software (Checklist 4A, line 5)**, and the **System configuration (Checklist 4A, lines 6-A through 6-E)**.

If the workstation might be more than a 300 foot cable run from the nearest communications closet, operate in a high electrical noise area, or otherwise benefit from 10BaseF connection, mark "YES" on **10BaseF NIC card required (Checklist 4A, line 6-F)**. If the user expects to send/receive many megabyte or larger files, mark "YES" on **FDDI NIC card required (Checklist 4A, line 6-G)**.

Gather information on the distribution of applications software used and the departments and work groups for which each LAN user works. For each LAN user for which the network application software usage can be ascertained record the location and programs used on the site survey copy of the floor plans. Identify **Common user program/data requirements. departments, or workgroups (Checklist 4B, line 2)**. Record the symbol used on the floor plan to show where each one is used.

EXAMPLE LAN DESIGN, Continued

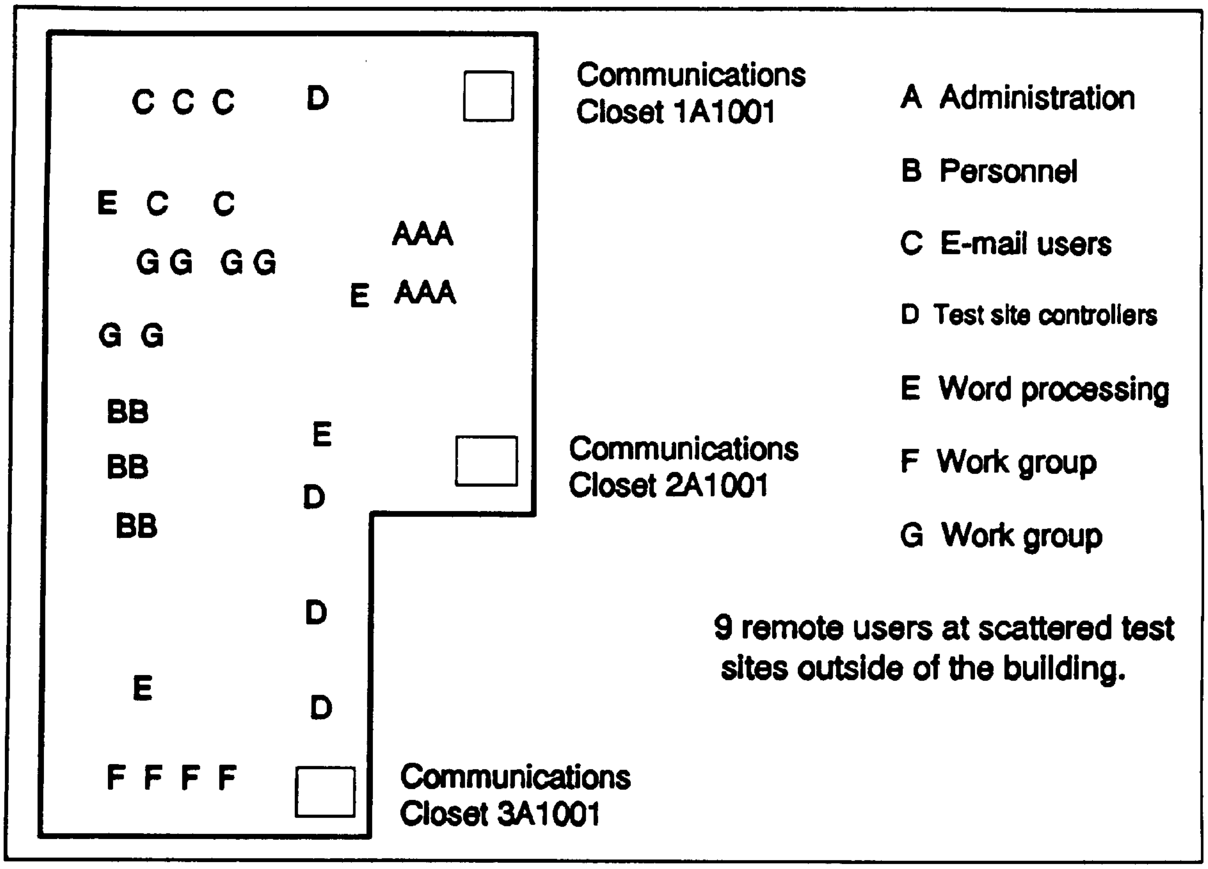
CONTINUATION OF EXAMPLE LAN DESIGN

Continuing the LAN design example from the survey team proceeds to survey the first floor of building 1001. During the preliminary site survey, the team marks the locations of the communications closets and user locations on the first copy of the floor plans. The floor plan with user locations for the LAN design example is shown in example figure 3.

The survey team completes Checklists 2A through 2C (example figure 4). The project name, Example LAN Design, is entered on line 1 of Checklist 2A. In line 2 the building to be served, 1001, is listed. Since there is only one building, only one copy of Checklist 2B is made. Line 1 repeats the project name (Example LAN Design). In this case, the building number of 1001 is entered on line 2-A to define which building contains the floors listed in 2-B. Line 2-B lists the first floor as the only floor in building 1001 to receive LAN equipment. With only one floor of one building being covered, only one copy of Checklist 2C is made. Line 1 lists the project name, Example LAN design. Line 2-A lists the building being described as 1001, and line 2-B lists the floor being described as the first floor. Line 2-C list the communications closets found on the first floor of building 1001. There are three communications closets found, with telephone equipment already installed. To illustrate the communications closet labeling technique, the closets are labeled 1A1001, 2A1001, and 3A1001, with communications closet 2A1001 being the telco BDF.

A copy of Checklist 3 is made for each communications closet, and the information for line 1 and lines 3-A through 3-F are entered, using the same information from Checklist 1A lines 1-A through 1-G. The communications closet name or label used on Checklist 2C line 2-C is entered on line 2, and the approximate location of the communications closet on the floor in 3-D. The survey team learns that no expansions of the telephone equipment are planned; therefore, any space found in the closets can be used for LAN equipment. There are no racks installed in the closets, a 0 is entered in each Checklist 3, line 4-A. There appears to be enough room to install one 80-inch high equipment rack with 72 inches of useable rack space in each closet, 72 inches is entered in each Checklist 3, line 4-B. Each communications closet is found to have a 4 inch opening in the ceiling, with only a few telephone cables currently installed in them. This leaves room for approximately 90 LAN cables to be installed in each closet before new openings are needed. Each Checklist 3, line 4-E's are marked to show room for no cables in the floor or walls, and 90 cables in the ceiling. Example figure 5 shows how information is recorded for communications closet 1A1001.

During the site survey, information on workstations was recorded in copies of Checklist 4A. An example completed form is found in example figure 6. While recording the workstation configuration for each user, the survey team also asks each intended LAN user about current and future software and data use. The team finds five main categories of users; administration, personnel, E-mail users, test site controllers, and word processing. See example figure 3. These categories will be represented by the symbols "A" for administration, "B" for personnel, “C” for E-mail, “D” for test site controllers, and "E" for word processing. The remaining users seem to form two work groups, and are labeled "F" and "G". These symbols and work groups are listed in Checklist 4B line 2. The completed Form 4B is shown in example figure 6.



EXAMPLE FIGURE 3. Floor plan with user locations.

SITE SURVEY CHECKLIST 2A
PROJECT DATA
(Make a copy for the LAN Project Manager.)

1. Survey Location Data
Name or number of LAN design project : *Example LAN Design*

2. List names or numbers of buildings to be served by this LAN project :

1001

EXAMPLE FIGURE 4. Stage 2 Checklist 2A.

SITE SURVEY CHECKLIST 2B
BUILDING FLOOR LOCATION DATA
(Make a copy for each building in LAN project.)

1. Survey Location Data
   Name or number of LAN design project : ___*Example LAN Design*___

2. Floors to be served by this LAN project
   A. Name or number of building containing these floors : ___*1001*___

   B. List of floors in building to be served by this LAN project:

   ___*First Floor*___

   ____
   ____
   ____
   ____
   ____
   ____
   ____
   ____
   ____
   ____
   ____
   ____
   ____
   ____
   ____

EXAMPLE FIGURE 4. Stage 2 Checklist 2B. - cont.

SITE SURVEY CHECKLIST 2C
FLOOR COMM CLOSET LOCATION DATA
(Make a copy for each floor in each building in LAN project.)

1. Survey Location Data
Name or number of LAN design project : *Example LAN Design*

2. List of Communications closets
A. Name or number of building containing these comm closets : *1001*

B. Number of floor in building containing these comm closets : *First Floor*

C. List of communications closets on this floor

Communications closet name	Approximate location
1A1001	*North East Corner*
2A1001 (BDF)	*Middle of East Wall*
3A1001	*South East Corner*

EXAMPLE FIGURE 4. Stage 2 Checklist 2C. - cont.

SITE SURVEY CHECKLIST 3
COMMUNICATIONS CLOSET TABLE
(Make a copy for each Comm Closet.)

1. Survey Location Data
Name or number of LAN design project : *Example LAN Design*

2. Label or name for communications closet : *1A1001*

3. Location of Communications closet
   A. Post : *Fort Redrock*
   B. Building : *1001*
   C. Floor : *First Floor*
   D. Approximate location : *North East Corner*
   E. Date prepared : *09/30/93*
   F. Name of preparer : *DOIM*
   Telephone number : *555-1000*

4. Current physical and electrical capacities
   A. Unused rack/cabinet space (vertical inches) : *0*
   B. Potential rack/cabinet space : *72 inches*
   C. Number of unused 20 amp power circuits available for LAN use : *1*
   D. HVAC : Additional ventilation required? Yes / No *NO*
   E. Cable routing capacity (estimated number of additional cables)
   Floor : *0*
   Ceiling : *90 CABLES*
   Walls : *0*
   Cable routing obstructions in closet? Yes / No *NO*
   F. Lockable door to communications closet or lockable electronics cabinet? Yes / No *NO*

EXAMPLE FIGURE 5. Stage 2 Checklist 3.

SITE SURVEY CHECKLIST 3
COMMUNICATIONS CLOSET TABLE

5. User Loads
   A. Communications closet region floor area : ____________________
   B. Maximum number users per closet : ____________________
   C. Initial user count : ____________________
   D. 10BaseF connectors : ____________________
   E. FDDI connectors : ____________________

6. Equipment Loads
   A. User cable length needed (feet) : ____________________
   B. Comm closet to BDF fiber optic cable length : ____________________
   C. UTP module count for maximum number of users : ____________________
   D. UTP module count for initial users : ____________________
   E. 10BaseF module count : ____________________
   F. FDDI module count : ____________________
   G. Maximum I/O module count : ____________________
   H. Number of full sized hubs needed : ____________________
   I. Number of small hubs needed : ____________________
   J. Number of local bridges needed : ____________________
   K. UTP patch panels needed : ____________________
   L. UTP patch panel rack space needed : ____________________
   M. Fiber optic patch panels needed : ____________________
   N. Fiber optic patch panel rack space needed : ____________________
   O. Number of backbone cables needed : ____________________
   P. Backbone cable needed : ____________________
   Q. Rack space needed : ____________________

EXAMPLE FIGURE 5. Stage 2 Checklist 3. - cont.

SITE SURVEY CHECKLIST 3
COMMUNICATIONS CLOSET TABLE

7. Additional physical and electrical requirements
   A. Additional rack/cabinet space needed : ____________________

   B. Additional number of racks or cabinets needed : ____________________

   C. Additional 20 amp single load circuits needed : ____________________

   D. Additional HVAC ventilation needed : ____________________

   E. Additional cable routing needs
      (number, size, location) : ____________________

   F. Add lockable door or lockable cabinets : ____________________

8. BDF Only
   A. Number of Bridges in the building : ____________________

   B. Number of 10BareF modules : ____________________

   C. Number of FDDI modules : ____________________

   D. Number of small hubs : ____________________

   E. Number of large hubs : ____________________

   F. Number of FO patch panels : ____________________

   G. Rack space for small hubs : ____________________

   H. Rack space for large hubs : ____________________

   I. FO patch panel rack space for backbone : ____________________

   J. Total number of building backbone cables : ____________________

   K. Total rack space needed : ____________________

   L. Additional rack/cabinet space needed : ____________________

   M. Additional number of racks or cabinets needed : ____________________

EXAMPLE FIGURE 5. <u>Stage 2 Checklist 3</u>. - cont.

SITE SURVEY CHECKLIST 4A
USER WORKSTATIONS

1. Survey Location Data
Name or Number of LAN design project : *Example LAN Design*

2. User name and location : *PFC Wright room 157*

3. Network services needed

A. E-mail services required? Y / N *YES*

B. File server space needed (Megabytes) : *15*

C. Network printer services needed? Y / N *YES*

D. Network communications services
Dial-Up line required? Y / N *NO*

FAX services required? Y / N *NO*

Direct terminal connection needed? Y / N *NO*

E. Network Applications
Word processing? Y / N *YES*

Spreadsheet processing? Y / N *NO*

Database processing? Y / N *NO*

Other office automation applications? Y / N *NO*

F. Other software applications used

Part of Administration work group SYMBOL "A"

EXAMPLE FIGURE 6. Stage 2 Checklist 4A.

SITE SURVEY CHECKLIST 4A
USER WORKSTATIONS

4. Workstation type :
   A. IBM PC [ ]
   B. IBM PC compatible [X]
   C. Apple Macintosh [ ]
   D. Other [ ]
   specify : ____________________

5. Operating system software
   A. MS DOS [X]
   version : 3.3
   B. Macintosh OS [ ]
   version : ____________________
   C. UNIX [ ]
   POSIX compliant? Yes / No
   version : ____________________
   D. Other [ ]
   specify : ____________________ version : ____

6. System configuration
   A. Main memory (MegaBytes) : 0.512

   B. Disk storage capacity (Megabytes) : 20

   C. Expansion bus type
   ISA 8 bit [ ]
   ISA 16 bit [X]
   EISA [ ]
   MCA [ ]
   NuBus [ ]
   Other [ ]
   specify : 3

   D. Number of unused expansion slots : ____________________

   E. Existing Ethernet interface [ ] NO
   UTP [ ]
   BNC (thinnet) [ ]
   AUI (thicknet) [ ]
   Fiber optic (ST) [ ]
   Other [ ]
   specify : ____________________

   F. 10BaseF NIC card required? Yes / No NO

   G. FDDI NIC card required? Yes / No NO

EXAMPLE FIGURE 6. Stage 2 Checklist 4A. - cont.

SITE SURVEY CHECKLIST 4B
APPLICATIONS OR DEPARTMENT SYMBOLS

1. Survey Location Data
Name or number of LAN design project : *Example LAN Design*

2. Common user program/data requirements, departments, or work groups

Symbol	Application or Department Name
A	*Administration*
B	*Personnel*
C	*E-mail Users*
D	*Test Site Controllers*
E	*Word Processing*
F	*Work Group 1*
G	*Work Group 2*

EXAMPLE FIGURE 6. Stage 2 Checklist 4B. - cont.

STAGE 3 - PRELIMINARY SITE SURVEY DATA ANALYSIS

GENERAL

At this stage, the preliminary site survey data will be used to determine which communications closet locations will be used to provide adequate LAN coverage. The communications closet region boundaries are then refined. The floor plan will be used to select user information drop locations. The design team needs Site Survey Checklists, 1 through 3, completed in Stages 1 and 2; the floor plans used in the preliminary site survey; and the second and third copies of the floor plans.

DETERMINE COMMUNICATION CLOSET COVERAGE

On the second copy of the floor plans, mark and label the locations of all the communications closets listed on Checklist 2C. The communications closets will initially be assumed to contain one LAN hub each. The design team will then determine if any communications closets do not need a LAN hub, and if any additional communications closets are needed to hold additional LAN hubs in sparse areas. The goal is to have each user drop within a 300 foot cable run of a LAN hub, and each LAN hub covering a region of 10,000 square feet or less.

Estimate area

Estimate the floor area served by the LAN hub in each communications closet to find any regions larger than 10,000 square feet or smaller than 5,000 square feet. Consider only areas to be covered by the LAN. Do not make precise measurements yet, as the communications closet regions have not yet been chosen.

Combine small areas

If there are adjacent communications closet regions with a combined total of less than 10,000 square feet which still maintain less than 300 foot cable lengths to all LAN users, consider combining the areas served and eliminating the LAN hub from one of the communications closets. Retain the LAN hubs in the communications closets that are the most ready to support LAN equipment. Do not combine if both closets are too small or too crowded to support large patch panels and hubs, or if running user cable to cover both regions from a single closet is impractical.

Split up large areas

Based on the cable routing impediments marked on the floor plans, it may be cost effective to separate some communications closet regions into smaller units. This will occur when a portion of the area served by a LAN hub extends across a cabling impediment, such as a firewall or crowded hallway. In these cases, consider breaking up the region, and perhaps adding a communications closet and LAN hub on the other side of the cabling impediment to avoid running user cable across this barrier. Also break up regions of more than 10,000 square feet, as they may require more rack space for hubs and patch panels than can fit into some communications closets.

Verify coverage

Using the second copy of the site survey floor plans, measure the cable run lengths with a ruler calibrated to the scale of the floor plan drawings. Make sure that allowances are made for going up and down walls, turning corners, and going around obstacles. In lieu of precise cable run measurements, use a 200 foot radius circle around each communications closet on scale drawing floor plans.

Figure 3-9 shows a possible building floor plan with three communications closet regions defined. For clarity, the floor plan is repeated three times so that only one 200 foot radius circle, centered on a communications closet, is drawn on each copy. Note that the middle communications closet has a far corner where users may be out of reach of normal 10BaseT cable distance. These users should either be re-assigned to the right-hand communications closet, connected with FOIRL, 10BaseF, or FDDI to the middle closet, or assigned to a fourth region with a small hub that will serve those users.

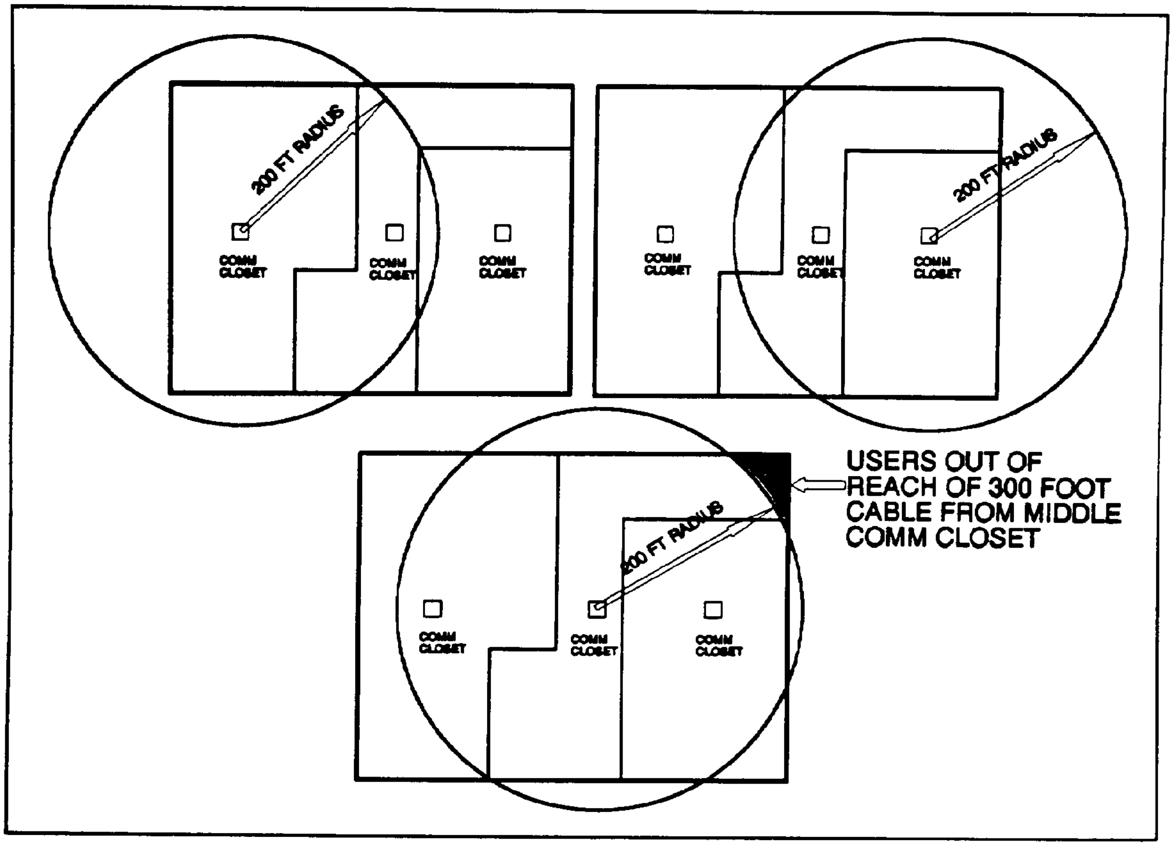


FIGURE 3-9. Possible floor plan with 200 foot radius circles.

The 200 foot radius is used to estimate the distance cable will go when routed up and down walls and around comers. Buildings with severe cable routing restrictions or no scale drawings may require more detailed coverage mapping.

If cable runs in excess of 300 feet will be installed for 10BaseF or FDDI connections, label them clearly as unsuitable for 10BaseT use.

CAUTION: Use of even one over-length 10BaseT connection can cause all users on the same hub or subnet to fall or operate intermittently. Strict adherence to Ethernet timing requirements and cable Installation standards is essential to ensure reliable network operation. Custom designs that meet the Ethernet

timing requirements but that violate the cabling standards may be difficult to document and maintain.

Verify that all LAN users and all future service areas are within the 300 foot cable length or 200 foot radius circles of a LAN communications closet. Most LAN user locations should be within at least two circles to allow flexible layout. Identify LAN users who are not likely to be within a 300 foot cable run, and mark their location on the second copy of the site survey floor plan. During the final phase of the site survey, they must be checked carefully for cable run length to see if fiber optic connections will need to be used.

Add LAN communications closets

If more than 10 LAN users are in an area outside of the circles of the communications closets, consider identifying a new communications closet to cover the area and add it to the site survey forms. If 10 or fewer LAN users are more than 300 feet and less than 3000 feet from a communications closet, or there are more than 10 users but they are widely dispersed, FOIRL or 10BaseF can be used to connect them.

If any LAN users are more than 3000 feet from the nearest communications closet, refer to section 2 of this document for remote LAN user connection techniques.

REFINE COMMUNICATION CLOSET BOUNDARIES

It is important to clearly define to which communications region of service of one communications closet and the region of service of the adjacent communications closet will simplify installation and maintenance of the user cabling. Regional boundaries which combine work groups and common users will minimize building backbone data traffic.

Categorize LAN users

Use the list of common LAN user applications, departments, and work groups on Checklist 4B, and the locations marked on the floor plans, to group LAN users together into communicans closet regions. These regions will often follow departmental boundaries. See figure 3-10 for an example floor plan with data included.

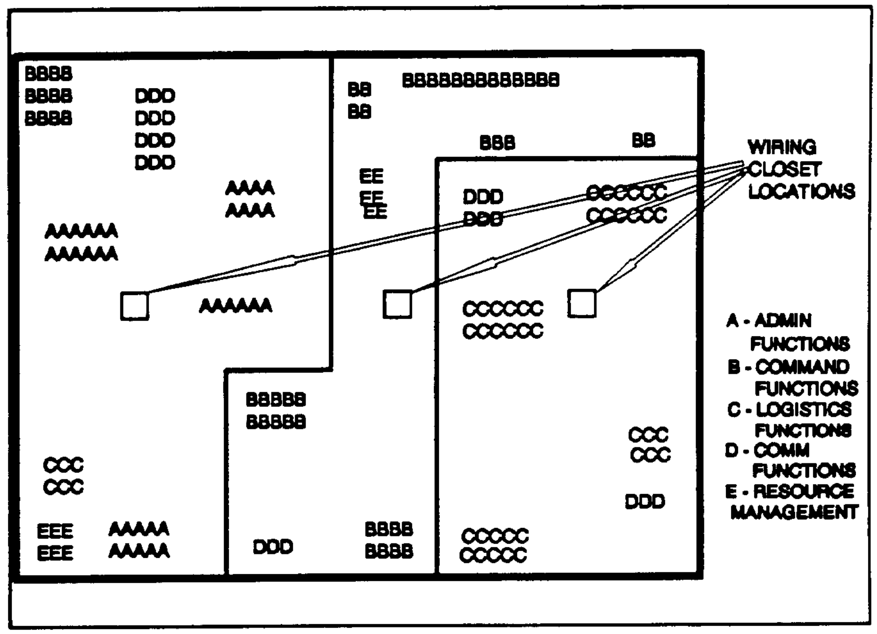


FIGURE 3-10. Example map of common user applications, departments, and work groups.

Define communications closet boundaries

Using the LAN user locations on the site survey floor plans, refine the communications closet regions. Try to keep LAN sers of the same programs, departments, or work groups within a single communications closet region. Placing servers in the communications closet to which the user is connected will minimize backbone usage.

Do not make the boundaries too complex, as this will make lon g-term LAN maintenance more difficult. Since LAN users may move from location to location, and application usage may change, the regions will eventually become mixed, anyway. If LAN user application usage data is not available, or the LAN users are mixed together, use simple floor plan boundaries to define the departmental regions.

If a BDF communications closet has already been identified, decide whether it should only provide backbone connectivity or if it should also provide LAN user connectivity. This determination will be based on the amount of rack space available in the BDF closet and whether adjacent regions can easily support LAN users near the BDF. Identify the closet as the BDF communications closet, **Label or name for communications closet (Checklist 3, line 2).**

Verify departmental boundaries

Verify that each departmental boundary lies wholly within the 300 foot cable run or 200 foot radius area of coverage of its communications closet. If any information drops are more than a 300 foot cable length from a communications closet, the out of range information drops must be reassigned to nearer communications closet(s) and the departmental boundaries modified to reflect the reassignment. Once the departmental boundaries have been finalized, copy them onto the communications closet floor plan (copy 2 of the floor plans). The final departmental boundaries will define the communications closet regions.

Maximum number of Users per Communications closet

To estimate the **Maximum number of users per closet (Checklist 3, line 5-B),** measure and record the **Communications closet region floor area (Checklist 3, line 5-A).** Divide the communications closet region floor area, Checklist 3, line 5-A, by 40 square feet and multiply by 1.2. For small rooms or partitions, use a minimum of two user information drops per room to allow flexible positioning of network equipment. See figure 3-11.

$$\begin{matrix}\textit{maximum number}\\ \textit{of users per closet}\end{matrix} = 1.2 * \left(\frac{floor_{sq.\ feet}}{40_{sq.\ feet}}\right)$$

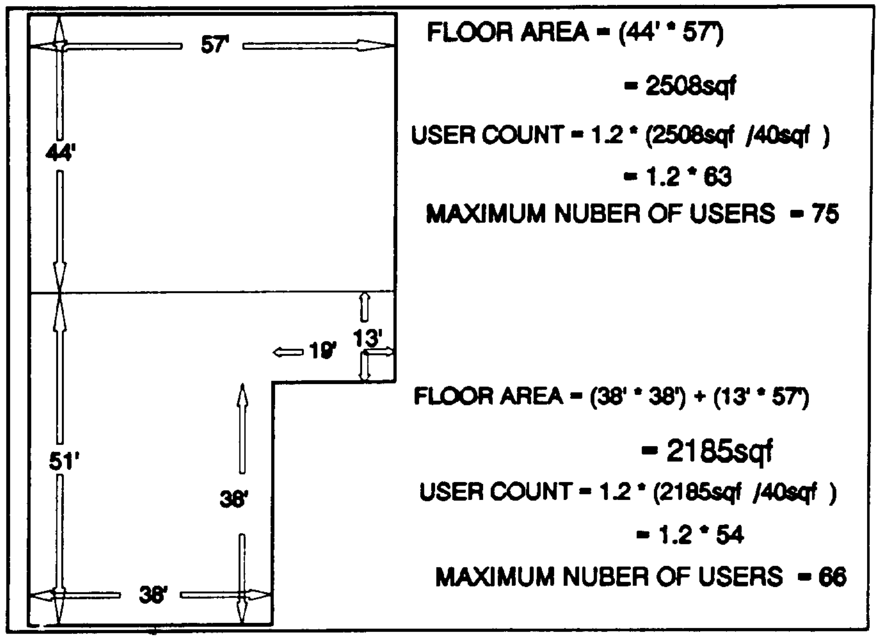


FIGURE 3-11. Maximum number of users.

Using the user location information in the site survey floor plans and workstation location data (Checklist 4A), combine user workstation forms into communications closet regions. Include any servers (Checklist 1B) whose final location is known. Determine the number of initial users in each communications closet region. Record the **Initial user count (Checklist 3, line 5-C)** in each closet. For each initial user, check the information on Checklist 4A, lines 6-F and 6-G, to see if 10BaseF or FDDI connections should be made. For each communications closet region, total all **10BaseF connections (Checklist 3, line 5-D)** required for the respective closet. For each communications closet region, total all possible **FDDI connections (Checklist 3, line 5-E)** required for the respective closet. Be sure to include any servers in the FDDI count. The FDDI count will only be used in the Hybrid/FDDI design.

IDENTIFY USER DROP LOCATIONS

For each communications closet region, get the maximum number of LAN users from Checklist 3, line 5-B. Mark the user drop location on the floor plan to show the wall plate or information drop location for each of the maximum number of LAN users. The drops should be evenly spaced to cover all areas where a LAN user may need to connect to the LAN.

For hallways, stairwells, utility closets, and other non-office space, find a suitable location for the wall plate. This will allow for later floor plan changes and new information drop uses such as communications, environmental controls, fire alarms and detectors, and surveillance and security. Verify that an ending location for every user cable for each communications closet has been marked, so that the total hybrid cable length for each communications closet will be correct.

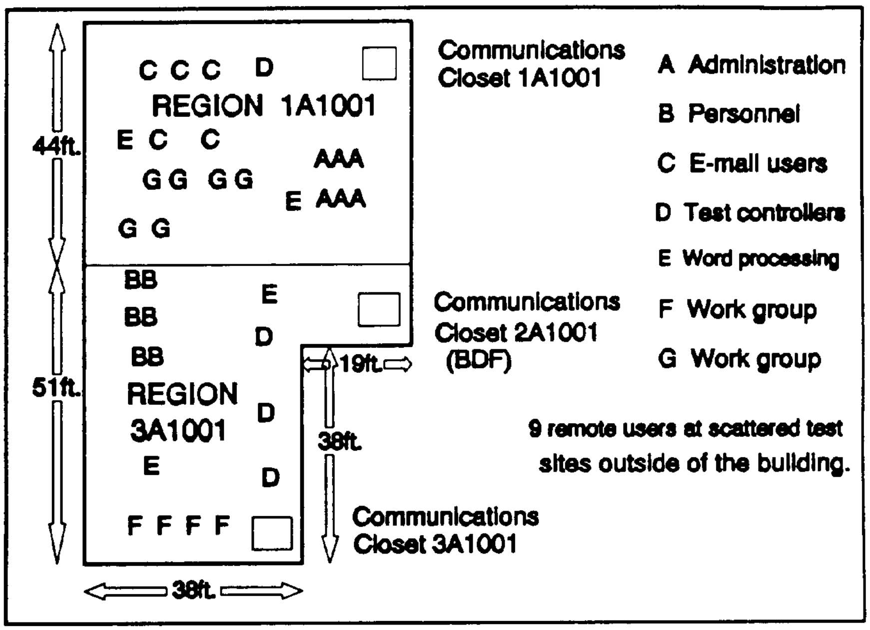
EXAMPLE LAN DESIGN, Continued

Continuing the example LAN design from the survey team has previously identified 3 communications closets, 35 LAN users within the building, and 9 LAN users at scattered test sites outside of the building. In the preliminary site survey analysis phase, the design team finds that the three communications closet regions have approximate areas of 1600,1600, and 1500 square feet. This means that any two adjacent regions can be combined. If all three regions are combined into one, the combined total of maximum LAN users may require two hubs. Installing the two hubs in separate communications closets will result in less crowded conditions and easier cable maintenance. Since the BDF closet does not have enough room to install a rack for the BDF hub and a second rack for a LAN user connection hub, the design team decides to not use the BDF closet for user hubs. User hubs will be installed in the first and third communications closets.

The design team finds that all areas within the building can be reached with a 300 foot cable from any communications closet, and that no cable running impediments were found. There is no need to provide additional communications closets.

The nine remote LAN users identified during the preliminary site survey are noted on the drawings for a special check during the final site survey to see if a 3000 foot cable will reach them for 10BaseF connection.

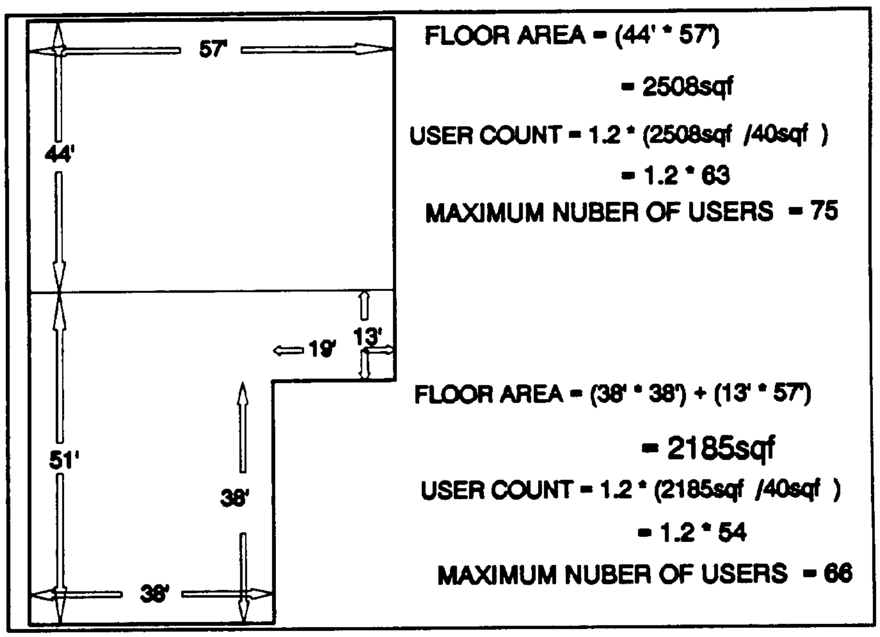
The LAN user locations on the first copy of the floor plan show that most LAN user groups are near each other; only the "E" group is spread out. A departmental boundary between communications closets 1A1001 and 3A1001 is then drawn to include the “B”, “D”, and "F" groups in region 3A1001, and the “A,” "C," and "G" groups in region 1A1001. The floor plan with departmental boundaries added is shown in example figure 7.



EXAMPLE FIGURE 7. Floor plan with region boundaries.

The floor plan is then measured to find the area of each communications closet region. See example figure 8. In region 1A1001, the area is 44 feet by 57 feet, with a total of 2508 square feet. The region area of 2508 is entered in Form 3, line 5-A, for closet 1A1001. In region 3A1001, the area consists of a 38 by 38 foot section and a 13 by 57 foot section. These total 2185 square feet. The total region area of 2185 is entered in Checklist 3, line 5-A for closet 3A1001.

The maximum LAN user count for region 1A1001 is 2508 divided by 40, times 1.2. This gives 75 user information drops needed for region 1A1001 The maximum user count of 75 is entered in the 1A1001's Checklist 3, line 5-B. In region 3A1001, the maximum LAN user count is 2185 divided by 40, times *1.2.* This gives 66 user drops in region 3A1001. The maximum user count of 66 is entered in the 3A1001's Checklist 3, line 5-B. The total number of user drops for the entire LAN is 75 plus 66 plus 9 remote LAN users, for a total of 150.



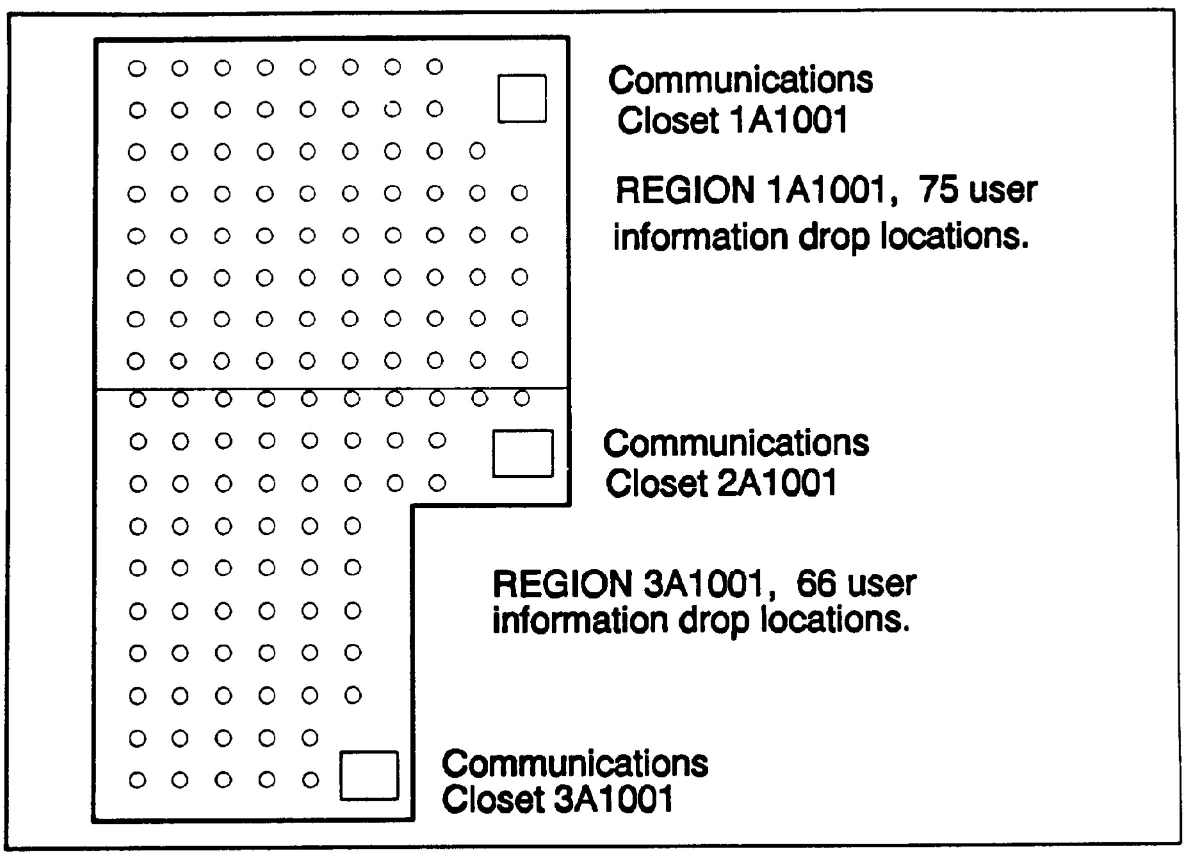
EXAMPLE FIGURE 8. Floor plan with region areas.

The user workstation Checklists 4As are separated into groups for regions 1A1001 and 3A1001. Counting the number of users in each region shows 20 initial users in region 1A1001 and 15 in region 3A1001. The initial user counts are then entered in each Checklist 3, line 5-C. Checking Checklist 4A, lines 6-F and 6-G, for each initial user, only the nine remote users will need 10BaseF connection, and no users were able to justify FDDI connection. Checklist 3 for closet 1A1001 shows the nine

10BaseF users on line 5-D, and zero FDDI connections on line 5-E. Checklist 3 for closet 3A1001 shows no 10BaseF or FDDI connections.

The third copy of the floor plans is then used to define the user information drop locations. The locations are spaced evenly over the floor area, such that there are 75 locations in region 1A1001 and 66 in region 3A1001. The third copy of the floor plans with the user drop locations is shown in example figure 9.

Checklist 3 for communications closet 1A1001 is shown in example figure 10.



EXAMPLE FIGURE 9. Floor plan with user drop locations.

SITE SURVEY CHECKLIST 3
COMMUNICATIONS CLOSET TABLE
(Make a copy for each Comm Closet.)

1. Survey Location Data
Name or number of LAN design project : *Example LAN Design*

2. Label or name for communications closet : *1A1001*

3. Location of communications closet
A. Post : *Fort Redrock*

B. Building : *1001*

C. Floor : *First Floor*

D. Approximate location : *North East Corner*

E. Date prepared : *09/30/93*

F. Name of preparer : *DOIM*

Telephone number : *555-1000*

4. Current Physical and Electrical Capacities
A. Unused rack/cabinet space (vertical inches) : *0*

B. Potential rack/cabinet space : *72 inches*

C. Number of unused 20 amp power circuits available for LAN use : *1*

D. HVAC : Additional ventilation required? Yes / No *NO*

E. Cable routing capacity (estimated number of additional cables)
Floor : *0*

Ceiling : *90 cables*

Walls : *0*

Cable routing obstructions in closet? Yes / No *NO*

F. Lockable door to communications closet or lockable electronics cabinet? Yes / No *NO*

EXAMPLE FIGURE 10. Stage 3 Checklist 3.

SITE SURVEY CHECKLIST 3
COMMUNICATIONS CLOSET TABLE

5. User Loads
   A. Communications closet region floor area : 2508 square feet
   B. Maximum number users per closet : 75
   C. Initial user count : 20
   D. 10BaseF connectors : 9
   E. FDDI connectors : 0

6. Equipment Loads
   A. User cable length needed (feet) : ______
   B. Comm closet to BDF fiber optic cable length : ______
   C. UTP module count for maximum number of users : ______
   D. UTP module count for initial users : ______
   E. 10BaseF module count : ______
   F. FDDI module count : ______
   G. Maximum I/O module count : ______
   H. Number of full sized hubs needed : ______
   I. Number of small hubs needed : ______
   J. Number of local bridges needed : ______
   K. UTP patch panels needed : ______
   L. UTP patch panel rack space needed : ______
   M. Fiber optic patch panels needed : ______
   N. Fiber optic patch panel rack space needed : ______
   O. Number of backbone cables needed : ______
   P. Backbone cable needed : ______
   Q. Rack space needed : ______

EXAMPLE FIGURE 10. Stage 3 Checklist 3. - cont.

SITE SURVEY CHECKLIST 3
COMMUNICATIONS CLOSET TABLE

7. Additional Physical and Electrical Requirements
   A. Additional rack/cabinet space needed : ______
   B. Additional number of racks or cabinets needed : ______
   C. Additional 20 amp single load circuits needed : ______
   D. Additional HVAC ventilation needed : ______
   E. Additional cable routing needs (number, size, location) : ______
   F. Add lockable door or lockable cabinets : ______

8. BDF Only
   A. Number of bridges in the building : ______
   B. Number of 10BaseF modules : ______
   C. Number of FDDI modules : ______
   D. Number of small hubs : ______
   E. Number of large hubs : ______
   F. Number of FO patch panels : ______
   G. Rack space for small hubs : ______
   H. Rack space for large hubs : ______
   I. FO patch panel rack space for backbone : ______
   J. Total number of building backbone cables : ______
   K. Total rack space needed : ______
   L. Additional rack/cabinet space needed : ______
   M. Additional number of racks or cabinets needed : ______

EXAMPLE FIGURE 10. Stage 3 Checklist 3. - cont.

STAGE 4 - BACKBONE/USER CABLING SITE SURVEY

GENERAL

In the final stage of the site survey, the survey team measures or estimates user and backbone cable lengths. Copies of floor plans two and three (COMMUNICATIONS CLOSETS and USER DROP LOCATIONS) and the Site Survey Checklist, Checklist 3 (Communications Closet Table), are required to complete Stage 4. All Checklists and floor plans used in Stage 4 should have been created in earlier stages. The actual quantity of cable necessary in the LAN design is addressed later in Stage 5, using the length requirements identified in the cabling portion of the site survey described below.

Total user cable length required per communications closet

To determine the total length of user cable required, sketch the proposed cable routes between each communications closet and related user drop locations on copy 3 (USER DROP LOCATIONS) of the floor plans. Section 4 of this document includes recommendations on cable routing techniques. Cable length can be determined by one of two methods:

- One, the survey team can physically measure each user cable path in the building, using a measuring tape or test length of wire or cable. This requires routing the measuring tape or cable along the same route that each user cable will run, including in conduits, cable trays, up and down walls, etc. Add 30 feet to the length of each cable to ensure sufficient length for actual installation. This method produces the most accurate results, but is very time consuming.

- Two, the survey team can use a baseline value of 230 feet per LAN user, averaged over all LAN users. This baseline value is high, but without detailed measurements of a specific site, a large baseline value is the only way to ensure that adequate amounts of user cable are purchased.

In the first method, to determine the **Total user cable (Checklist 3, line 6-A)** length required for each communications closet region, add user cable measurements together. with the second method, multiply the maximum number of users per closet (Checklist 3, line 5-B) by 230 feet. It is not necessary to record the individual cable lengths, as the cable will be cut to length as needed during the installation process.

Backbone cable length per communications closet

To determine each departmental **Communication closet to BDF backbone cable length (Checklist 3, line 6-B)**, identify the backbone cable routes and mark them on the second (COMMUNICATIONS CLOSETS) copy of the floor plans. Using the same procedures outlined above, measure or estimate the backbone cable length needed for each departmental communications closet to connect with the BDF, and add 30 feet to each run to ensure adequate length.

EXAMPLE LAN DESIGN, Continued

CONTINUATION OF EXAMPLE LAN DESIGN

Continuing the example LAN design from page 3-57, the project leader, not having the manpower necessary to measure each user cable run, decides to use the 230 foot baseline for each user cable length. The total user cable needed for region 1A1001 equals 230 feet times 75 (the maximum number of users per closet in region 1A1001), for a total user cable length of 17,250 feet,

$$USER\ CABLE = 230ft\ per\ user * 75\ users\ for\ region\ 1A1001$$
$$USER\ CABLE = 230ft * 75$$
$$USER\ CABLE = 17250\ feet$$

and 230 times 66 (the maximum user count in region 3A1001) for a total of 15,180 feet of cable in region 3A1001. The total of 15,180 feet of user cable needed in region 3A1001 is recorded in Checklist 3, line 6-A.

USER CABLE =* 230*ft per user* * 66 users for region 3*A1001
***USER CABLE =* 230*f*t * 75**
USER CABLE =* 15180 *feet

The cable needed for the remote test sites totals 18,000 feet of cable, and is added to the communications closet region 1A1001 total. The combined total of 35,250 feet of user cable for region 1A1001 is recorded in Checklist 3, line 6-A.

The two backbone cables going from the BDF to communications closets 1A1001 and 3A1001 are estimated from the floor plan to be 110 feet each. Adding 30 feet to each gives a total of 140 feet for each closet. Enter 140 for the communications closet to BDF cable length in Checklist 3, line 5-B, for regions 1A1001 and 3A1001. See example figure 11 for the region 1A1001 Checklist 3 with the cable measurements included.

SITE SURVEY CHECKLIST 3
COMMUNICATIONS CLOSET TABLE
(Make a copy for each Comm Closet.)

1. Survey Location Data
   Name or number of LAN design project : *Example LAN Design*

2. Label or name for communications closet : *1A1001*

3. Location of communications closet
   A. Post : *Fort Redrock*

   B. Building : *1001*

   C. Floor : *First Floor*

   D. Approximate location : *North east Corner*

   E. Date prepared : *09/30/93*

   F. Name of preparer : *DOIM*

   Telephone number : *555-1000*

4. Current Physical and Electrical Capacities
   A. Unused rack/cabinet space (vertical inches) : *0*

   B. Potential rack/cabinet space : *72 inches*

   C. Number of unused 20 amp power circuits available for LAN use : *1*

   D. HVAC : Additional ventilation required? Yes / No *NO*

   E. Cable routing capacity (estimated number of additional cables)
   Floor : *0*

   Ceiling : *90 cables*

   Walls : *0*

   Cable routing obstructions in closet? Yes / No *NO*

   F. Lockable door to communications closet or lockable electronics cabinet? Yes / No *NO*

EXAMPLE FIGURE 11. Stage 4 Checklist 3.

SITE SURVEY CHECKLIST 3
COMMUNICATIONS CLOSET TABLE

5. User Loads
   - A. Communications closet region floor area : *2508 square feet*
   - B. Maximum number users per closet : *75*
   - C. Initial user count : *20*
   - D. 10BaseF connectors : *9*
   - E. FDDI connectors : *0*

6. Equipment Loads
   - A. User cable length needed (feet) : *35,250 feet*
   - B. Comm closet to BDF fiber optic cable length : *140 feet*
   - C. UTP module count for maximum number of users : ____
   - D. UTP module count fo- initial users : ____
   - E. 10BaseF module count : ____
   - F. FDDI module count : ____
   - G. Maximum I/O module count : ____
   - H. Number of full sized hubs needed : ____
   - I. Number of small hubs needed : ____
   - J. Number of local bridges needed : ____
   - K. UTP patch panels needed : ____
   - L. UTP patch panel rack space needed : ____
   - M. Fiber optic patch panels needed : ____
   - N. Fiber optic patch panel rack space needed : ____
   - O. Number of backbone cables needed : ____
   - P. Backbone cable needed : ____
   - Q. Rack space needed : ____

EXAMPLE FIGURE 11. Stage 4 Checklist 3. - cont.

SITE SURVEY CHECKLIST 3
COMMUNICATIONS CLOSET TABLE

7. Additional Physical and Electrical Requirements
   A. Additional rack/cabinet space needed : ______________________
   B. Additional number of racks or cabinets needed : ______________________
   C. Additional 20 amp single load circuits needed : ______________________
   D. Additional HVAC ventilation needed : ______________________
   E. Additional cable routing needs (number, size, location) : ______________________
   F. Add lockable door or lockable cabinets : ______________________

8. BDF Only
   A. Number of bridges in the building : ______________________
   B. Number of 10BaseF modules : ______________________
   C. Number of FDDI modules : ______________________
   D. Number of small hubs : ______________________
   E. Number of large hubs : ______________________
   F. Number of FO patch panels : ______________________
   G. Rack space for small hubs : ______________________
   H. Rack space for large hubs : ______________________
   I. FO patch panel rack space for backbone : ______________________
   J. Total number of building backbone cables : ______________________
   K. Total rack space needed : ______________________
   L. Additional rack/cabinet space needed : ______________________
   M. Additional number of racks or cabinets needed : ______________________

EXAMPLE FIGURE 11. Stage 4 Checklist 3. - cont.

STAGE 5 - CREATE LAN DESIGNS

GENERAL

This stage is a step-by-step procedure for a LAN design based on the results of the site survey process performed in stages 1 through 4. If you are reading this document for informational purposes only, and do not have site specific survey data, it is not necessary to complete any of the site survey checklists during these steps. For reference, at the end of this stage, the running example illustrates the process with specific data.

Stage 5 addresses BDF and departmental communications closet and building backbone designs for the four performance variations based upon vendor hub design (identified in stage 5) and the site survey data collected previously. Also included are procedures for selecting the LAN's network operating system, network servers, UPSs, and network interface cards (NICs). In addition to all previously used forms and floor plans, a copy of checklist 5 (LAN Design Worksheet) is required to complete stage 5

DEPARTMENTAL COMMUNICATION CLOSET/HUB DESIGN

It is important to note again that a departmental communications closet and BDF communications closet can be one in the same, depending upon on whether or not the BDF communications closet contains a hub for user connection to the backbone. In either case, design for user connection to the backbone (the departmental communications closet) is the same. The only difference is that the backbone connecting the departmental hub(s) and the BDF hub(s) is contained within the one closet.

The departmental communications closet electronics includes the intelligent hubs, SNMP management and bridging modules needed in each hub, and the I/O modules needed for user interface with the hub. Any servers that may be placed in the closet will be addressed later in this design stage. The hub count in each closet is based on the number of I/O modules needed to support the maximum number of users, and the hub capacity. The number of I/O modules needed depends on the maximum user count and the I/O module capacities. The hub and I/O module capacities depend on the hub vendor selected. The communications closet electronics design proceeds from hub vendor selection to hub count for each communications closet.

Hub vendor selection

A hub vendor must be selected from the CCL for both the basic hub and the multiport bridging hub. If a hub vendor is not selected at this time, the baseline values given below must be used. In either case, the first step is to complete Checklist 5, lines 2-A through 2-G and 2-L, (basic hub capacities) for reference in later steps. If a hub vendor is selected, copy the hub and module capacities from the CCL into Checklist 5, lines 2-A through 2-G and 2-L.

Baseline Hub Capacities

If a hub vendor cannot be selected at this time, the following baseline values should be used.

- **UTP connections per module (Checklist 5, line 2-A),** use a baseline of 12.

Some vendors will support 24 or even 48 UTP connections in a single module, but these modules are typically more than one slot wide. They also often use 50-pin telco connectors to concentrate more connections on one card; these are more noise sensitive than many separate RJ-45 connectors.

- **10BaseF connections per module (checklist 5, line 2-B),** use a baseline of 12.

- **FDDI connections per module (Checklist 5, line 2-C),** use a baseline of six FDDI single-attach connections. This ranges between two and eight for various vendors.

Remember that most vendors will support one dual-attach connection in place of two single-attach connections. It is assumed that most LAN user equipment will not need a dual-attach connection. However, in the Ethernet/FDDI and Hybrid/FDDI LAN designs with a FDDI backbone, the connections between hubs WILL be dual-attach, so that only three departmental communications closet hubs will be able to attach to each FDDI module in the BDF hub.

- **<u>110 modules per full-sized hub (Checklist 5, line 2-D),</u>** use a baseline of nine.

- **<u>110 modules per small hub (Checklist 5, line 2-E),</u>** use a baseline of four.

- **<u>Vertical rack space needed per full-sized hub (Form 5. line 2-F),</u>** use a baseline of 20 inches.

- **<u>Rack space needed per small hub (Checklist 5, line 2-G)</u>**, use a baseline of 14 inches.

- **<u>Number of ports in multiport bridging hub (Checklist 5, line 2-L)</u>**, use a baseline of 20 ports.

Figure 3-12 illustrates a possible Ethernet/FDDI LAN hub co,. figuration. The hub configuration shown requires an Ethernet SNMP module, an FDDI SNMP module, and an FDDI-to-Ethernet bridging module. These three modules would leave nine slots free in a 12 slot hub.

Some vendors may combine some of these functions into two or even just one module; the number of slots available may vary, as well.

Compute I/O module counts

To compute the number of I/O modules needed in each departmental communications closet (including the BDF. closet if user connections must be supported there), the design team will need the module capacities now entered in Form 5 and the user connection needs in each Checklist 3.

UTP module count for maximum number of users

Determine the **<u>UTP module count for maximum number of users (Checklist 3, line 6-C)</u>** for each departmental communications closet; divide the maximum number of users per closet (Checklist 3, line 5-B) (current, planned, and anticipated) by the UTP connections per module (Checklist 5, line 2-A), and round upward.

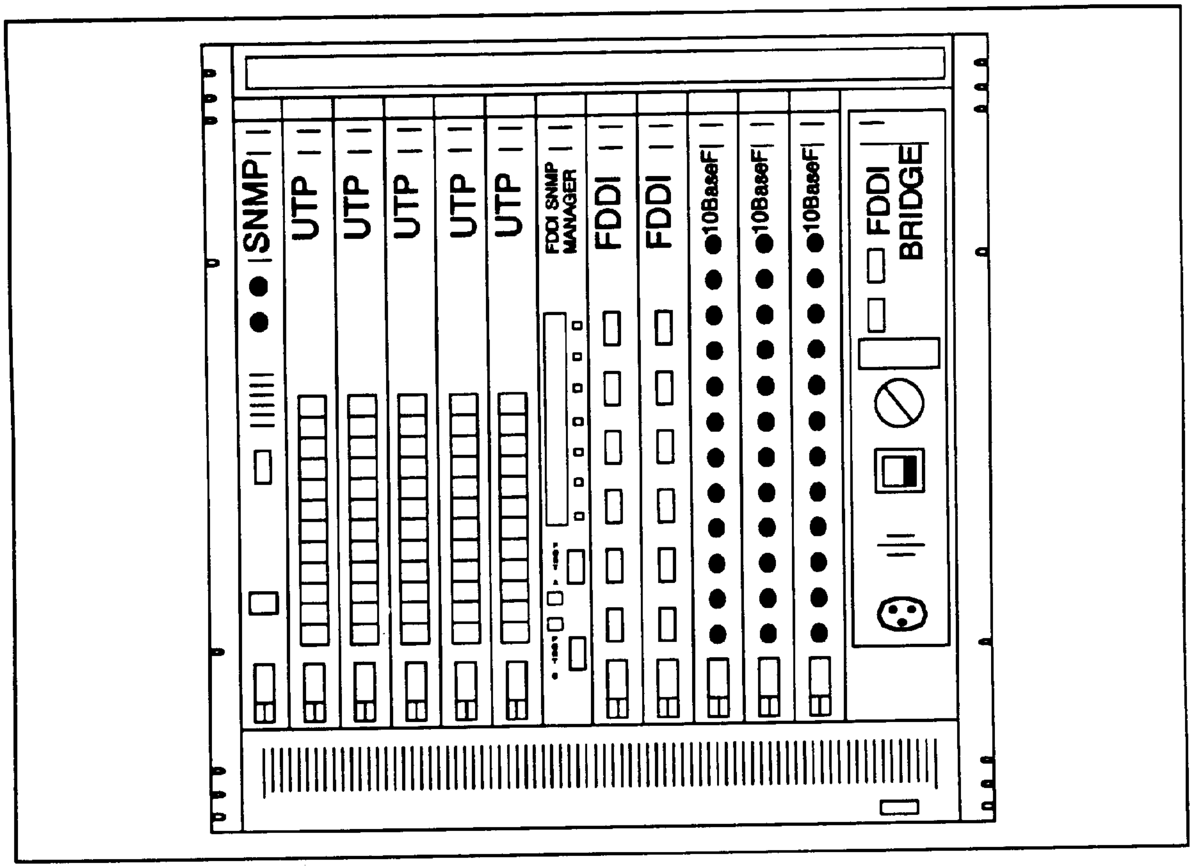


FIGURE 3-12. Possible Ethernet/FDDI hub configuration.

$$UTP\ MODULE\ COUNT = ROUND\ UP\ \left(\frac{MAX\ USER\ COUNT\ PER\ CLOSET}{UTP\ CONNECTIONS\ PER\ MODULE}\right)$$

UTP module count for initial users

Determine the **UTP module count for initial users (Checklist 3, line 6-D)** for each departmental communications closet; divide the initial user count (Checklist 3, line 5-C) by the UTP connections per module (Checklist 5, line 2-A), and round upward.

The intelligent hub count will depend on the number of modules needed to support the maximum number of users, but the cost estimate and initial LAN equipment purchase will only include I/O modules for initial users.

Calculate the **<u>Total number of UTP modules needed (Checklist 5, line 3-A)</u>** for all departmental communications closets; total the UTP module count for initial users (all Checklist 3, line 6-D) for all departmental communications closets.

10BaseF module count

Determine the **<u>10BaseF module count (Checklist 3, line 6-E)</u>** for each departmental communications closet; divide the 10BaseF connections (Checklist 3, line 5-D) by the 10BaseF connections per module (Checklist 5, line 2-B), and round upward. If a closet does not have any 10BaseF users, enter zero in Checklist 3, line 6-E.

$$\text{10BaseF MODULE COUNT} = \text{ROUND UP}\left(\frac{\text{10BaseF USER CONNECTIONS}}{\text{10BaseF CONNECTIONS PER MODULE}}\right)$$

Calculate the **<u>Total number of 10BaseF modules for user connections (Checklist 5, line 3-C)</u>** to all departmental communications closets; total the 10BaseF module count (all Checklist 3, line 6-E) for all departmental communications closets.

FDDI module count

FDDI user connections will only be used in the Hybrid/FDDI LAN design. To determine the **<u>FDDI module count (Checklist 3, line 6-F)</u>**, divide the FDDI connections (Checklist 3, line 5-E) for each departmental communications closet by the FDDI connections per module (Checklist 5, line 2-C), and round upward. If a closet does not have any anticipated FDDI users, enter zero in Checklist 5, line 2-C.

$$\text{FDDI MODULE COUNT} = \text{ROUND UP}\left(\frac{\text{FDDI USER CONNECTIONS}}{\text{FDDI CONNECTIONS PER MODULE}}\right)$$

Determine the **Total number of FDDI modules for user connections (Checklist 5, line 3-E)** for all departmental communications closets; total the FDDI module count (all Checklist 3, line 6-F) for all departmental communications closets.

Compute intelligent hub count

Each departmental communications closet defined in the site survey and analysis phases contains one or more intelligent hubs. If the BDF closet supports user connections, a separate hub will be used for user connections and for backbone connections, with a local bridge between them. Although some of the hubs will initially be sparsely populated, enough hubs will be installed to handle the maximum number of LAN users. This makes future growth easier. Communications closets with small regions may only need a small hub to handle all LAN users.

Determine the **Maximum I/O module count (Checklist 3, line 6-G)** to be supported in each departmental communications closet; add together the UTP module count for maximum number of users (Checklist 3, line 6-C), 10BaseF module count (Checklist 3, line 6-E), and FDDI module count (Checklist 3, line 6-F) in each departmental communications closet.

Checklist 5, lines 2-D and 2-E have the number of user 110 modules supported by a full-sized hub and a small hub, respectively.

Determine the **Number of small hubs needed (Checklist 3, line 6-I)**, and the **Number of full-sized hubs needed (Checklist 3, line 6-H)** that will support the required 110 modules in each departmental communications closet; compare the maximum I/O module count (Checklist 3, line 6-G) with the number of I/O modules per full-sized hub (Checklist 5, line 2-D) and the number of I/O modules per small hub (Checklist 5, line 2-E). If the number of I/O modules is less than or equal to the capacity of a small hub, use a single small hub for that closet. If the number of I/O modules required exceeds the capacity of a small hub, use a full-sized hub. If the number of I/O modules required exceeds the capacity of a full-sized hub, use a full-sized hub and a small hub.

To determine the **Number of local bridges needed (Checklist 3, line 6-J)** in each departmental communications closet, add the number of small hubs needed (Checklist 3, line 6-I) to the number of full-sized hubs needed (Checklist 3, line 6-H) in each departmental communications closet.

Patch panels

Select a vendor for the UTP and fiber optic patch panels from the CCL. A different vendor for each can be selected. Once a vendor has been selected, copy the UTP and fiber optic patch panel capacities into Checklist 5, lines 2-H to 2-K.

If a vendor is not selected for the UTP patch panel, use a baseline for **UTP connections per patch panel (Checklist 5, line 2-H)** of 48, and a baseline for **Rack space needed per UTP patch panel (Checklist 5, line 2-I)** of 3.5 inches. For the fiber optic patch panel, use a baseline for **ST connections per fiber optic patch panel (Checklist 5, line 2-J)** of 96, and a baseline for **rack space needed per panel (Checklist 5, line 2-K)** of 7 inches.

There are usually several different sizes of UTP patch panels, but this will give a good estimate of the amount of rack height needed to accommodate all the UTP patch panels. Fiber optic patch panels come in a variety of sizes and connector styles. The ST connectors were chosen for their ease of use and commonality. Patch cables are available to convert ST connections into most other connector styles, as needed. These smaller patch panels can be used instead of full-sized panels to save money if a full-sized panel would end up with few connections.

Compute patch panel counts

To determine the number of **UTP patch panels needed (Checklist 3, line 6-K)** for each departmental communications closet, multiply the maximum user count per closet (Checklist 3, line 5-B) by 2 connections per cable, and then divide that number by the connections per

UTP patch panel (Checklist 5, line 2-H), and round upward.

$$\textit{UTP PATCH PANEL COUNT} = \textit{ROUND UP}\left(\frac{2 * \textit{MAX USER COUNT PER CLOSET}}{\textit{UTP CONNECTIONS PER PATCH PANEL}}\right)$$

To determine the amount of **UTP patch panel rack space needed (Checklist 3, line 6-1)** for each departmental communications closet, multiply the UTP patch panels needed (Checklist 3, line 6-K) per closet by the rack space needed per UTP patch panel (Checklist 5, line 2-I).

To determine the number of **Fiber optic patch panels needed (Checklist 3, line 6-M)**, multiply the maximum user count in the closet (Checklist 3, line 5-B) times 4. Add 12 backbone cable connections for each small or full-sized hub and then divide by the number of ST connections per fiber optic path panel (Checklist 5, line 2-J).

$$\textit{FIBER OPTIC PATCH PANEL COUNT} = \textit{ROUND UP}\left(\frac{4 * \textit{MAX USER COUNT} + 12 * \textit{HUB COUNT}}{\textit{FIBER OPTIC CONNECTIONS PER PANEL}}\right)$$

To determine the amount of **Fiber optic patch panel rack space needed (Checklist 3, line 6-N)**, multiply the FO patch panels needed (Checklist 3, line 6-L) per closet, by the rack space needed per FO patch panel (Checklist 5, line 2-K).

Determine the **Total number of UTP patch panels (Checklist 5, line 5-A)** needed in all closets; total the number of UTP patch panels needed (all Checklist 3, line 6-K) in all departmental communications closets.

Compute rack space needed

To determine the total **Rack space needed (Checklist 3, line 6-Q)** for each departmental communications closet, total the patch panel rack space requirements (Checklist 3, lines 6-L and 6-N), and add the rack space needed for the hubs (Checklist 3, line 6-H times Checklist 5, line 2-F plus Checklist 3, line 6-I times Checklist 5 line 2-G).

Compare the existing unused rack space (Checklist 3, line 4-A) and potential additional rack space (Checklist 3, line 4-B) with the rack space required to install the additional equipment. For any closet without enough installed rack space, indicate the **Additional rack/cabinet space needed (Checklist 3, line 7-A), Additional number of racks or cabinets needed (Checklist 3, line 7-B),** and/or other installation procedures required.

For each departmental communications closet, compare the number of separate ac power circuits available for LAN hubs (Checklist 3, line 4-C) with the total number of hubs to be installed in the closet (Checklist 3, line 6-H plus Form 3, line 6-I). Record the **Additional 20 amp single load circuits needed (Checklist 3, line 7-C)**.

Compare the estimated number of cables that can be added to existing openings in the floor, walls, and ceiling of each departmental communications closet (sum of Checklist 3, lines 4-E) to the maximum user count (Checklist 3, line 5-B). If more cable openings are needed, or the existing openings will not support the preferred cable routing paths, indicate the **Additional cable routing needs (Checklist 3, line 7-E)** for new ducts/openings (number, size, and location).

If additional ventilation is required (Checklist 3, line 4-D) in a closet, indicate the **Additional HVAC ventilation needed (Checklist 3, line 7-D)**. If a closet is without a lockable door (Checklist 3, line 4-F), indicate the need to **Add lockable door or lockable cabinets (Checklist 3, line 7-F)**, instead of open racks.

Any upgrade work needed before installation of LAN equipment should be spelled out in the Site Concurrence Memorandum, and responsibility for completing each upgrade should be assigned. The Site Concurrence Document is discussed further in section 4.

If any communications closet is found to be too sm all, it may be necessary to resurvey the area. Check to see if there are ways to expand the communications closet or install more additional rack space. It may also be possible to switch to a different communications closet in the same area or redraw the communications closet region to decrease the floor space in this communications closets region, and thus reduce the maximum number of LAN users. It may also be possible to create an additional communications closet to take some of the load. If any changes are made in the communications closet locations or regions, you must also resurvey the user cable routing and lengths. Before leaving the site after the final site survey, make sure that each communications closet can handle the LAN equipment that will be added, and that the communications closet tables, floor plans, and cable routing needs reflect the current communications closet locations.

USER AND BACKBONE CABLE DESIGN

The inside cable plant design consists of totaling all the cable needed to support the maximum user count and the backbone cable needed to support each departmental communications closet. Cable will be ordered in bulk and cut to length during installation.

User cable requirements

Determine the **Total amount of user cable needed (Checklist 5, line 6-A)** for the LAN design; total the user cable needs for all departmental communications closets (all of Checklist 3, line 6-A) and multiply by 1.2 to add extra cable for spares.

Backbone cable requirements

Each departmental communications closet will receive a strands for each LAN hub in the closet. Closets with only one hub need only one backbone cable, closets with two or three hubs need two cables, etc. To find the **Number of backbone cables needed (Checklist 3, line 6-O)** for each departmental communications closet, multiply the total number of local bridges in the closet (Checklist 3, line 6-J) by 8 strands per hub, divide by 12 stands per cable and round upward.

$$\text{BACKBONE CABLE COUNT PER COMM CLOSET} = \left(\frac{\text{HUB COUNT} * 8 \text{ STRANDS PER HUB}}{12 \text{ STRANDS PER CABLE}}\right)$$

Any extra strands will be terminated and saved for future expansion. Find the total length of **Backbone cable needed (Checklist 3, line 6-P)** for each departmental communications closet to connect with the BDF, then multiply the departmental communications closet to BDF fiber optic cable length (Checklist 3, line 6-B) by the total number of backbone cables needed (Checklist 3, line 6-O) in the closet.

Compute the **Total number of building backbone cables (BDF Checklist 3, line 8-J)**; total the number of backbone cables needed for all departmental communications closets (all Checklist 3, line 6-O).

Determine the **Total amount of Backbone cable (Checklist 5, line 6-B)** needed for the LAN design; total the backbone cable needed (Checklist 3, line 6-O) for all departmental communications closets, and multiply by 1.2 to add extra cable for spares.

BUILDING BDF COMM CLOSET/ BACKBONE DESIGN

For networks of two user connection hubs or less, a BDF backbone hub may not be necessary. Backbone cable routing should still come to a central BDF closet to allow for future expansion. If no building BDF hub exists in the design, only the BDF backbone patch panel needs to be designed. Ensure that one copy of Checklist 3 has been identified as the BDF communications closet (Checklist 3, line 2) for design purposes. This copy of the Checklist will be referred to as the “BDF Checklist 3."

To design the backbone, one of the four recommended LAN design variations must be selected. Each variation adds greater performance and usually greater cost. The primary difference between each variation is in the type of interface used on the building backbone. The BDF backbone hub, if needed, can either be the same type used in the departmental communications closets or a multiport bridging hub, depending upon the variation used.

- **Basic Ethernet/Ethernet** - In this LAN design, there is an Ethernet connection for each LAN user and an Ethernet connection between each departmental communications closet and the BDF hub with a local bridge in each departmental communications closet.

- **Multiport Ethernet/Ethernet** - This LAN design provides an enhancement to the Basic Ethernet/ Ethernet by using a multiport bridging hub for the BDF. The higher internal bandwidth of the bridging hub's backplane provides greater performance than a standard Ethernet backbone, and eliminating the local bridges may more than offset the added cost of the bridging hub.

- **Ethernet/FDDI** - This design variation provides an Ethernet connection to the LAN users, but uses an FDDI-to-Ethernet bridge in each departmental communications closet for the backbone connection. The example LAN design presented at the end of each stage uses the Ethernet/FDDI variation.

- **Hybrid/FDDI** - This LAN design variation provides an FDDI connection to some LAN users and Ethernet to others. Because the LAN user connections are a mixture of two interfaces, this is labeled Hybrid/FDDI. Each departmental hub uses an FDDI-to-Ethernet bridge for the backbone connection. This is the only variation to have a difference in user connection.

All LAN design variations provide cost effective long-term operation and an easy upgrade path for high LAN capacities and new technology. It is also possible for the advanced installer to mix the performance variations although that is not recommended for those without network engineering experience.

Building backbone/hub design

The design of the building backbone varies depending on the number of departmental communications closets, the need for an intelligent hub in the BDF, and the performance variation chosen. For the following computations, determine the total **Number of bridges In the building (BDF Checklist 3, line 8-A)** for each building in the LAN design;

total all local bridges in each building (sum of Checklist 3, line 6-J). A BDF closet must have been selected from among the locations identified as communications closets at this point to continue with the design process.

The building backbone design depends on the backbone interface used and the size of the LAN. If there are more than 50 users, more than two hubs were identified, or an out of building connection is desired, an additional central hub will be needed. This hub will be designated the BDF hub and will interconnect all the other communications closets/hubs.

The location of the BDF and all the interconnect cabling should have been defined in the site survey and analysis steps. The BDF can be in the same communications closet as departmental hubs, as long as there is enough room for all the equipment. The BDF should be connected to the post-wide backbone with a router, even though local bridges are used inside the building. This will allow more advanced filtering and routing functions to take place on the post-wide backbone.

50 User LAN backbone

For the 50 user LAN, there should be at most two departmental communications closet hubs to interconnect, and no BDF hub. If there is only one intelligent hub supporting the LAN, no interconnection is needed. If there are two intelligent hubs in the LAN, connect the two bridging modules together with backbone fiber optic cable. See figure 3-13 for a 50 user network model using an FDDI backbone. The CUTIN interface, when needed, will be installed in the BDF closet and will probably necessitate the addition of a BDF hub.

If a BDF was identified in the site survey and a different cable route was shown, correct the drawings to show the new cable route. Alternatively, a third hub can be used for the BDF to allow for future expansion, but at a higher initial cost. The backbone fiber optic cable can also be routed to the BDF closet patch panel, and then connected together with patch cables. This will retain the star topology for the backbone cables and simplify a later addition of a BDF hub or connection to CUTIN.

If there are more than two hubs, refer to the 150 user LAN backbone design. Since there is no BDF hub in the 50 user network designs, there is no Multiport bridging variation.

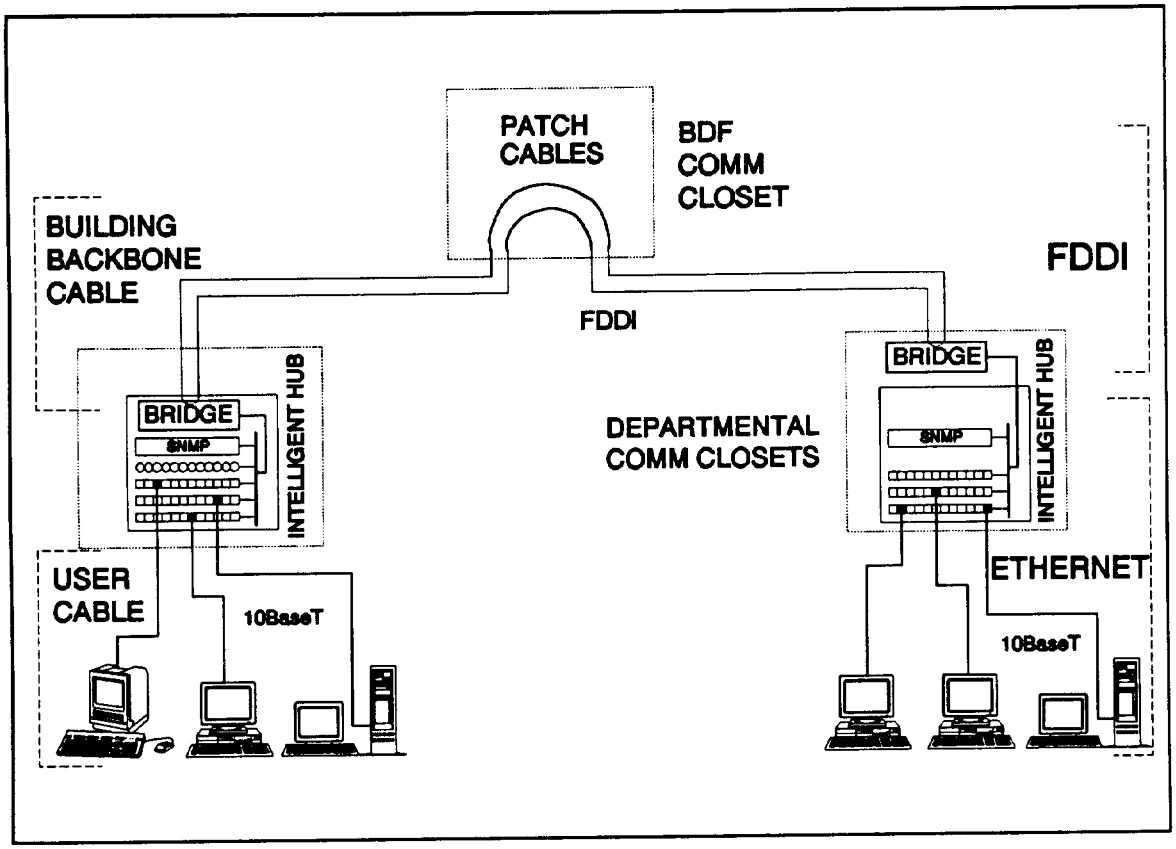


FIGURE 3-13. 50 user network model with FDDI backbone.

Ethernet/ Ethernet 150 User LAN backbone

For both the Basic Ethernet/Ethernet and Multiport Ethernet/Ethernet variations, the backbone uses 10BaseF connections between the BDF and each intelligent hub in each departmental communications closet. See figure 3-14 for a 150 user network model with an Ethernet backbone.

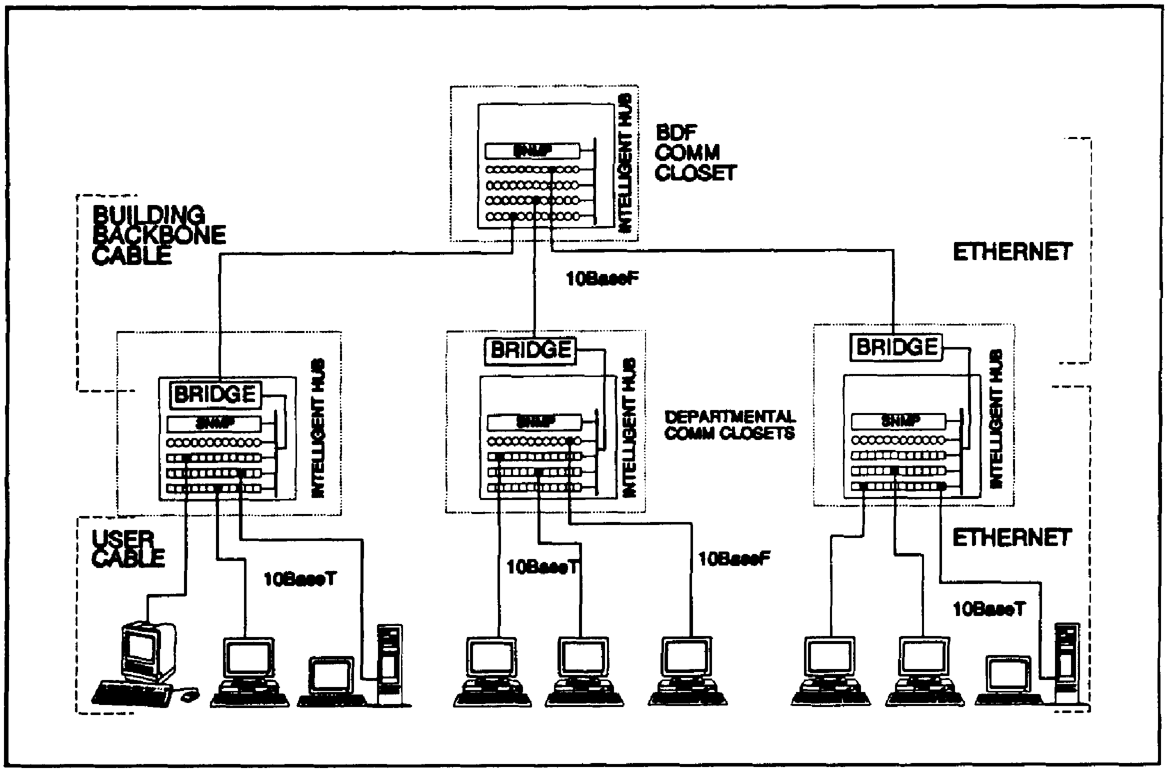


FIGURE 3-14. 150 user Ethernet backbone network model.

BDF hub, 10BaseF module count

To determine the **Number of 10BaseF Modules (BDF Checklist 3, line 8-B)** in a basic Ethernet/Ethernet variation BDF, divide the number of bridges in the building (BDF Checklist 3, line 8-A) by the number of 10BaseF connections per module (Checklist 5, line 2-B), and round up. A single small hub should be able to support all of these modules.

$$\text{BDF 10BaseF MODULE COUNT} = \text{ROUND UP}\left(\frac{\text{TOTAL BRIDGE COUNT}}{\text{10BaseF CONNECTIONS PER MODULE}}\right)$$

Record the **Total number of 10BaseF modules for backbone (Checklist 5, line 3-B)**, found in BDF Checklist 3, line 8-B. For any design with a BDF hub, leave one extra slot for a CUITN interface.

BDF multiport bridging hub count

To determine the **<u>Total number of multiport bridging hubs (Checklist 5, line 4-C)</u>** for the Multiport Ethernet/Ethernet variation, divide the number of bridges in the building (BDF Checklist 3, line 8-A), plus one for a CUITN connection, by the number of ports in a multiport bridging hub (Checklist 5, line 2-J), and round up.

$$\text{BDF MULTI-PORT BRIDGING HUB COUNT} = \text{ROUND UP}\left(\frac{\text{TOTAL BRIDGE COUNT} + 1}{\text{CONNECTIONS PER BRIDGING HUB}}\right)$$

If more than one hub is needed in the closet, allow one port on each hub to connect to each of the other hubs. See figure 3-15 for a 150 user network model with a multiport bridging hub in the backbone. Leave one extra port for the CUITN interface.

If more than two multiport bridging hubs are needed, consider using the Ethernet/FDDI or Hybrid/FDDI designs, instead. Record the number of multiport bridging hubs needed in BDF Form 3 and in Form 5. Leave at least one port open for an external router, or one slot for an internal router to connect to the post-wide backbone.

Ethernet/FDDI and hybrid/FDDI 150 user LAN backbone

For the Ethernet/FDDI and Hybrid/FDDI LAN variations, the backbone uses FDDI connections between the BDF and each intelligent hub in each departmental communications closet.

To determine the **<u>Number of FDDI modules (BDF Checklist 3, line 8-C)</u>** required in the BDF, multiply the number of bridges in the building (BDF Checklist 3, line 8-A) by 2 to allow dual-attach connections for each hub, divide by the number of connections in an FDDI module (Checklist 5, line 2-C), and round upward.

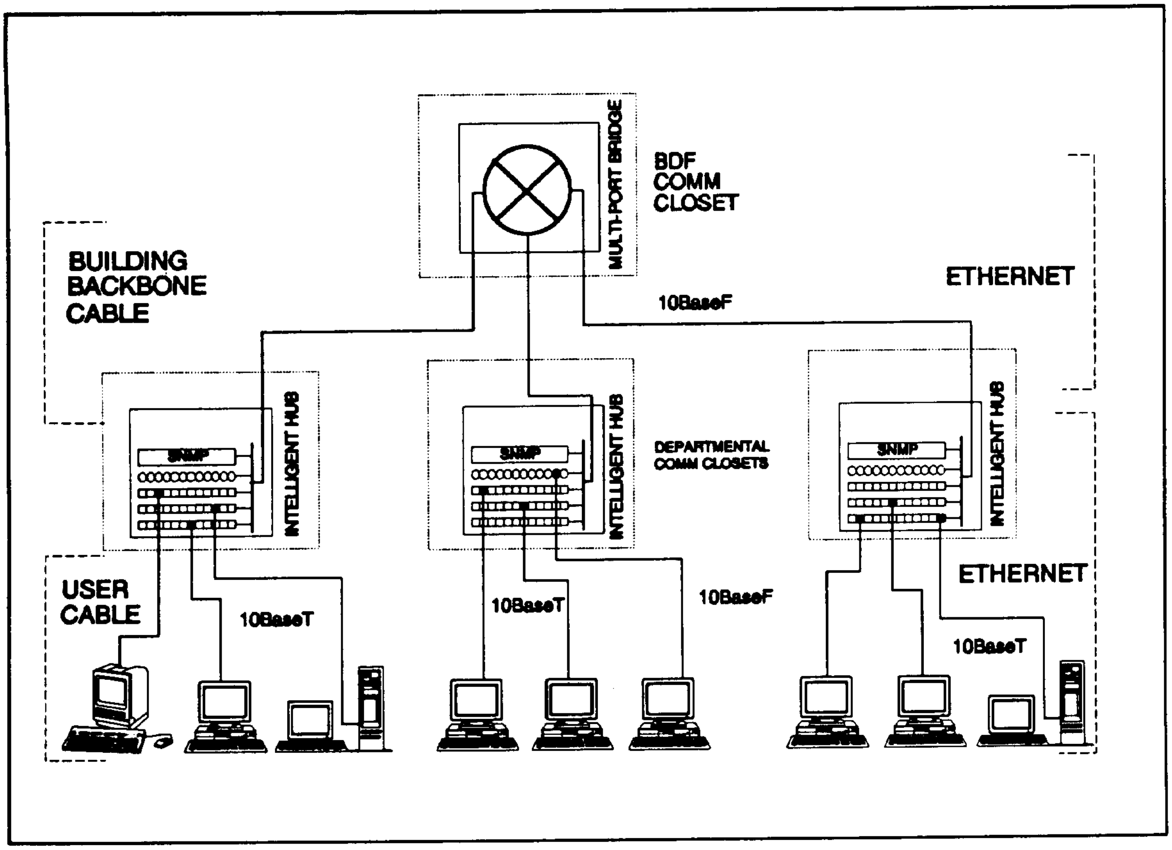


FIGURE 3-15. 150 user Multi-port Bridge backbone network model.

$$\textit{BDF FDDI MODULE COUNT} = \textit{ROUND UP}\left(\frac{\textit{TOTAL BRIDGE COUNT} * 2}{\textit{FDDI CONNECTIONS PER MODULE}}\right)$$

Record the **Total number of FDDI modules for backbone (Checklist 5, line 3-D)** found in BDF Checklist 3, line 8-C. See figure 3-16 for a 150 user Hybrid/FDDI network model.

Since the FDDI modules support fewer connections than the 10BaseF modules, a small hub might not suffice. Leave one slot open for future addition of a bridging/routing module to connect to the post-wide backbone.

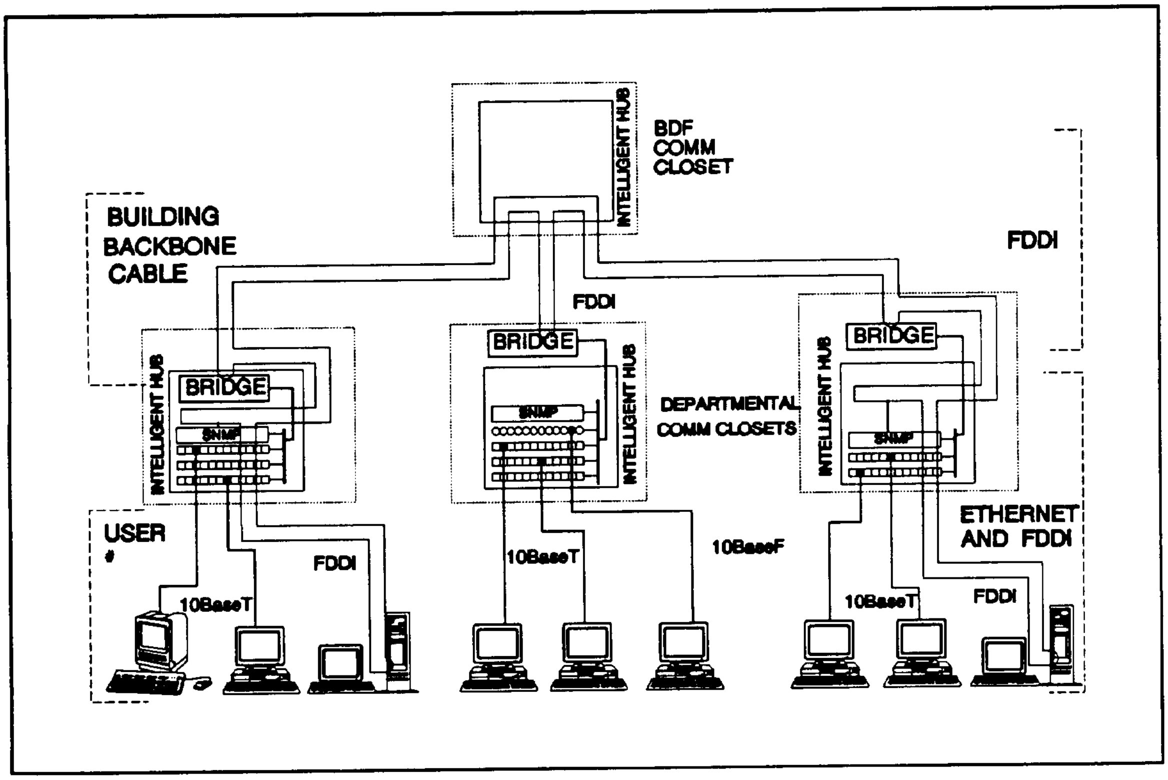


FIGURE 3-16. 150 user Hybrid/FDDI network model.

1000 User LANs or larger

The backbone techniques used in the 150 user LAN can also be used for the 1000 user LAN within a single building. The only difference will be that a small hub in the BDF closet is not likely to hold enough I/O modules to connect to each departmental hub, or that more than one hub may be needed. If additional hubs are needed, they should be connected to the first hub. A slot should be left open in the first hub to allow for connection to the post-wide backbone. If Class C Internet addresses will be used, it may also be necessary to use routers instead of bridges to allow segmentation of IP addresses into subnets of 255 or fewer workstations. Otherwise, follow the instructions for the 150 user LAN design described above.

For large LANs that cover more than one building, an inter--building network is needed. If such a network already exists, use the 150 user LAN interconnection technique to create a separate network for each building, and connect each building's BDF to the post-wide backbone with bridging or routing modules. If no such inter-building network exists yet, one must be created before the buildings can be connected. It is recommended that the CUITN model be used to design the post-wide backbone. Section 2 of this document describes inter-connection techniques.

BDF Intelligent hub count

The BDF closet design is based on the number of intelligent hubs in the departmental communications closets, the number of backbone cables needed, and the performance variation chosen. To facilitate future upgrades, the BDF hub(s) will be sized to handle either a 10BaseF or FDDI backbone.

To determine the number of BDF hubs (the **Number of small hubs (BDF Checklist 3, line 8-D)** and the **Number of lame hubs (BDF Checklist 3, line 8-E)**) in the Basic Ethernet/Ethernet and FDDI variations, take the number of backbone connection modules from BDF Checklist 3, line 8-B or 8-C, whichever is greater, and determine how many hubs are required. If direct user connections are required in the BDF closet, a separate hub will provide for user connections. This is accounted for in BDF Checklist 3, lines 6-A through 6-Q. The bridge to provide user hub to backbone connection is identified in line 6-J. Many LANs will only need one small hub for the BDF, unless there are many communications closets.

Identify the **Total number of small hubs (Checklist 5, line 4-B**) needed for the LAN design; add the total number of small hubs needed (Checklist 3, line 6-I) in the departmental communications closets to the number of small hubs needed in the BDF communications closet (BDF Checklist 3, line 8-D).

Identify the **Total number of full-sized hubs (Checklist 5, line 4-A)** needed for the LAN design; add the total number of full-sized hubs needed (Checklist 3, line 6-H) in all departmental communications closets to the number of large hubs needed in the BDF communications closet (BDF Checklist 3, line 8-E).

BDF patch panel requirements

For each backbone cable running into the BDF, there must be 12 fiber optic connections in the BDF patch panel. Therefore, to determine the **Number of fiber optic patch panels (BDF Checklist 3, line 8-F**) needed in the BDF, multiply the total number of building backbone cables (BDF Checklist 3, line 8-J) by 12, add 24 extra connections for any future outside plant cabling, and divide by the number of ST connections per fiber optic patch panel (Checklist 5, line 2-J).

$$\textit{FIBER OPTIC PATCH PANEL COUNT} = \textit{ROUND UP}\left(\frac{\textit{BACKBONE CABLE COUNT}*12 + 24}{\textit{ST PORTS PER PANEL}}\right)$$

Determine the **Total number of fiber optic patch panels (Checklist 5, line 5-B)** needed in all closets; add the total of fiber optic patch panels needed for user connection in all departmental communications closets (Checklist 3, line 6-M) to the number of fiber optic patch panels needed for backbone connection in the BDF (BDF Checklist 3, line 8-F).

The 24 spare ports for outside cable plant connections should be able to terminate single-mode fiber. The outside cable plant fiber optic cable may be the only single-mode fiber inside the building.

BDF closet rack space requirements

Compute the vertical **Rack space for small hubs (BDF Checklist 3, line 8-G)** needed for the BDF; multiply the number of small hubs (BDF Checklist 3, line 8-D) used for the BDF by the rack space needed per small hub (Checklist 5, line 2-G).

Compute the vertical **Rack space for large hubs (BDF Checklist 3, line 8-H)** needed for the BDF; multiply the number of large hubs (BDF Checklist 3, line 8-E) used for the BDF by the rack space needed per full-sized hub (Checklist 5, line 2-F).

Compute the vertical **Fiber optic patch panel rack space (BDF Form 3. line 8-I)** needed for the BDF; multiply the number of fiber optic patch panels needed (BDF Checklist 3, line 8-F) for the BDF by the rack space needed per fiber optic patch panel (Checklist 5, line 2-K).

Determine the **Total rack space needed (BDF Checklist 3, line 8-K)** for the BDF; compute the sum of the rack space required for the fiber optic patch panels (BDF Checklist 3, line 8-I), the small hubs (BDF Checklist 3, line 8-G), and the large hubs (Checklist 3, line 8-H) used for the BDF, and add enough extra space to support a BDF UPS (7 to 24 inches) along with a possible external routing device (5 to 14 inches).

Compare the existing unused rack space (BDF Checklist 3, line 4-A) and possible additional rack space (BDF Checklist 3, line 4-B) with the total required rack space (BDF Checklist 3, line 8-K). Indicate the **Additional rack/cabinet space needed (BDF Checklist 3, line 8-L)**, **Additional number of racks or cabinets needed (BDF Checklist 3, line 8-M)**, and/or other installation procedures required.

If there is insufficient rack space, make a special note to upgrade the BDF communications closet to provide enough rack space for all the equipment needed. The BDF hub is the only hub that does not require a UTP patch panel, unless it provides LAN user connections This will decrease the rack space requirements somewhat, so be sure to consider this when verifying the communications closet capacity.

NETWORK OPERATING SYSTEM

The network operating system (NOS) must be Government Open Systems Interconnections Profile (GOSIP) compliant, and must be interoperable with past government required standards, including support for TCP/IP. The NOS selected will determine which network servers, file servers, print servers, and NIC driver software will be compatible.

Although NOS specifications and analysis of current vendor offerings is still in progress, the following recommendations will help in determining the desirability and long-term interoperability of available NOS packages.

- The NOS should operate with standards-based driver software in the NICs of the user workstations, for example Network Driver Interface Specification (NDIS) or Open Data-link Interface (ODI). This will support commonality among networks and ease network integration.

- The client software running on the user workstations should support either or both the TCP/IP and TP4/CNLP protocol stacks. The server software must simultaneously support both protocol stacks and must provide full network services to each user without requiring them to switch protocol stacks.

- The NOS should provide a Network Basic Input/Output System (NetBIOS) interface to applications programs; this interface should be provided for both TCP/IP and TP4/CNLP communications.

- The NOS should support user workstations running MS-DOS, WINDOWS, WINDOWS NT, *OS/2,* and UNIX.

- The NOS and user workstation software should support communication with existing E-mail servers using the Server Message Block (SMB) protocol.

- The NOS must support the initial number of users for the LAN and should be upgradeable to support the maximum number of users.

Each of these recommendations is intended to simplify network configuration and operation and the user interface. If no NOS packages can be found that support all recommendations, a NOS that supports most is preferred. Select a NOS from the CCL. Once the NOS has been selected, consult the vendor or the vendor documentation to find the minimum server configuration (random access memory (RAM) size, disk size, processor speed, etc.) to run the NOS and support the initial users.

SERVERS

The type, quantity, and configuration of the servers needed was recorded in Checklist(s) 1B. LAN user needs were also surveyed and recorded in Checklist(s) 4A. Use table 3-I and the following server descriptions to further refine the server requirements. Additionally, the final decision will be dependent upon the chosen vendor. Select a vendor from the CCL to use in the costing of servers.

Network servers

The network server contains the NOS and LAN user passwords and access privileges and co-ordinates the operation of the LAN. Before selecting a network server, the NOS must be selected. The network server function is sometimes combined with the file server function in a single computer.

The number of LAN users per network server varies with NOS and server capacity. A maximum of 330 users per server is recommended using the guidelines in table 3-I. If a single computer performs both the network server and file server functions, then the computer should accommodate a maximum of 150 users. Research Form(s) 1B for requirements. Network server configurations and software are dependant on the NOS chosen. Consult the NOS vendor and documentation for recommendations. Enter the totals and costs for **Network servers (Checklist 5, line 7-A).**

TABLE 3-1. Typical server configurations.

SERVER =========== COMPONENT	NETWORK	FILE	APPLI-CATIONS	DATABASE	PRINT/ COMM
CPU	50 MHz 486 or 66 MHz DX2	50 MHz 486 or 66 MHz DX2	50 MHz 486DX or 66 MHz DX2	50 MHz 486DX or 66 MHz DX2	33 MHz 486
SYSTEM BUS	EISA or MCA	EISA or MCA	ISA	EISA or MCA	ISA
CACHE	64k	64k	256k	128k	64k
RAM	32 MB	24 MB	64 MB	64 MB	16 MB
DISK CAPACITY	600 MB	1 Gbyte	400 MB	600 MB	200 MB
DISK INTERFACE	SCSI-2	SCSI-2	SCSI-2	SCSI-2	IDE
POWER SUPPLY	250 Watts	250 Watts	200 Watts	250 Watts	200 Watts
INTERNAL SLOTS	4	4	4	4	8
BACKUP DEVICE	TAPE/ CD ROM	TAPE/ CD ROM	TAPE/ CD ROM	TAPE/ CD ROM	FLOPPY DISK

File servers

File server sizing is dependent on LAN user application needs. For each region, total the LAN user file space needs from each Checklist 4A, line 3-B, and add space for the selected operating system. Divide the total file space needed by the disk storage capacity of each file server in the configuration you choose. Enter the total and costs for **File servers (Checklist 5, line 7-B).**

If file space requirements are not available for all LAN users, an estimate of 10 Megabytes (MB) per LAN user may be used. It is also advisable to install extra capacity, as file space usage usually grows rapidly.

Applications servers

Applications servers, also called compute or process servers, run LAN user applications on a central computer, which might have faster processing and more memory, or allow many people to run the same program at one time. The requirements of the applications server are application specific. Research the application server requirements from each Checklist 1-B. Enter the total and costs for **Application servers (Checklist 5, line 7-C).**

Database servers

Database servers are just a special instance of applications servers that have been optimized to handle large database files. Database server requirements are application specific. Research the database server requirements from each Form 1-B. Enter the total and costs for **Database servers (Checklist 5, line 7-D).**

Print servers

Network printers can be connected to personal computer (PC) based network print servers, network file servers, individual LAN user workstations, or network printer controllers. The cost estimate in the next stage assumes laser printers and network printer controllers. For a standard office environment, use a baseline of 10 LAN users per printer. Document generation areas will need more printers; paperless office operations will not need as many. Network printer controllers typically control one or two laser printers. PC-based printer controllers, depending on operating system capabilities, can control up to 16 printers. Workstations typically only control one printer. Consult section 2 for further details on network printer connection and operation. if network print servers are required and laser printers are identified as network printers (Form(s) 1B), enter the totals and costs for **Print servers (Checklist 5, line 7-E).**

Communications servers

Depending on the application and needs, communications servers provide dial-up modems, ISDN connections, protocol conversion between networks, bridging and or routing functions between networks or network segments, connection to remote networks or users, and gateways to wide area networks (WAN)s. If communications servers are identified (Checklist(s) 1B), enter the totals and costs for **<u>Communication servers (Checklist 5, line 7-F)</u>.**

Refer to section 2 for further recommendations on communications servers, remote user and network access, protocol conversion, and gateway usage. For this network design, each network segment is connected with a dedicated bridging module, and the BDF connects to the post-wide backbone with a dedicated routing/bridging module.

E-mail servers

E-mail servers are an application server type with standard hardware/software configurations for Army purchase. Use a baseline of one E-mail server per 200 LAN users if the vendor does not provide a recommended users-per-server rate. Determine the number of E-mail servers needed. Enter the totals and costs for **<u>E-mail servers (Checklist 5, line 7-G).</u>**

UPSs required

Determine the total number of **<u>Uninterruptible power supplies (Checklist 5, line 8)</u>** for the LAN design, add up all the servers listed in Checklist 5, lines 7-A through 7-G, and add one UPS for each backbone hub in the BDF. Determine the **<u>Cost per UPS (Checklist 5, line 8)</u>**, by finding the cost of a UPS from the CCL.

NETWORK INTERFACE CARDS

The final step in the LAN design is to determine the number of user workstation NICs needed. To determine the **<u>Total number of 10BaseF NICS for initial users (Checklist 5, line 3-G)</u>**, count the number of 10BaseF NICs required (Checklist 4A, line 6-F).

To determine the **<u>Total number of FDDI NICs for Initial users (Checklist 5, line 3-H)</u>**, count the number of FDDI NICs required (Checklists 4A, line 6-G). To find the **<u>Total number of FDDI management/attach modules for Hybrid/FDDI (Checklist 5, line 3-I)</u>**, count the number of communications closets with one or more FDDI users.

To determine the **Total number of UTP NICs for initial users (Checklist 5, line 3-F)**, add the number of initial LAN users (Checklist 3, line 5-C) to the number of servers (total number of Checklists 1B), and then subtract the number of existing Ethernet interfaces - UTP (Checklists 4A, line 6-E) and subtract the number of 10BaseF cards.

If the type of existing Ethernet UTP interface card is unknown, it is recommended that a new NIC be installed. Older cards may cause interruptions and may not be interoperable. Also, for workstations that require a different NIC, consult the workstation vendor for availability and cost of NICs. For the servers listed in Form 1B, consider using 32-bit extended industry-standard architecture (EISA) bus NICs on servers that support the EISA bus interface.

EXAMPLE LAN DESIGN, Continued

Continuing the example LAN design, the design team now has all of the site survey data, and is ready to begin the LAN design stage. Full copies of the example checklists are presented in example figures 22 and 23. To further clarify the example design, fragments of each form are presented in the text where the information is discussed.

First, a copy of Checklist 5 is made and the project name is entered in line 1. The design team is not sure which vendors will be selected for the LAN equipment, so the baseline values from stage 5 for each capacity are copied into Checklist 5, lines 2-A through 2-L (see example figure 12).

The design team checks region 1A1001's Checklist 3, line 5-B, to find a maximum user count of 75. Using the UTP module equation from stage 5:

$$\mathit{UTP\ MODULE\ COUNT} = \mathit{ROUND\ UP}\ \left(\frac{\mathit{MAX\ USER\ COUNT\ PER\ CLOSET}}{\mathit{UTP\ CONNECTIONS\ PER\ MODULE}}\right)$$

With a maximum user count per closet of 75, and UTP connections per module of 12, the result of 7 UTP modules is entered in region 1A1001's Checklist 3, line 6-C.

$$7\ \mathit{UTP\ MODULES} = \mathit{ROUND\ UP}\ \left(\frac{75\ \mathit{USERS}}{12\ \mathit{USERS\ PER\ MODULE}}\right)$$

SITE SURVEY CHECKLIST 5
LAN DESIGN WORK SHEET

1. Survey Location Data
   Name or number of LAN design project : *Example LAN Design*

2. Design Capacities
   A. UTP connections per module : *12*
   B. 10BaseF connections per module : *12*
   C. FDDI connections (single attach) per module : *6*
   D. I/O modules per full-sized hub : *9*
   E. I/O modules per small hub : *4*
   F. Rack space needed per full-sized hub : *20*
   G. Rack space needed per small hub : *14*
   H. UTP patch panel connections per panel : *48*
   I. Rack space needed per UTP patch panel : *3.5*
   J. Fiber optic patch panel ST connections per panel : *96*
   K. Rack space needed per FO patch panel : *7*
   L. Number of ports in multi-port bridging hub : *20*

EXAMPLE FIGURE 12. Checklist 5 baseline values.

Region 1A1001's Checklist 3, line 5-C, shows 20 initial users. To reduce initial LAN costs, only enough UTP modules to support the initial users need be purchased. Using the same equation that was used for maximum user count, region 1A1001 has 20 initial users and 12 user connections per module. The result of 2 UTP modules for initial users is entered in line 6-D.

$$2\ \textit{UTP MODULES} = \textit{ROUND UP}\ \left(\frac{20\ \textit{USERS}}{12\ \textit{USERS PER MODULE}}\right)$$

Region 1A1001's Checklist 3, line 5-D, shows 9 10BaseF connections. Using the equation from stage 5:

$$\begin{matrix}\text{10BASEF}\\ \text{MODULE COUNT}\end{matrix} = \text{ROUND UP}\left(\frac{\text{10BASEF USER COUNT PER CLOSET}}{\text{10BASEF CONNECTIONS PER MODULE}}\right)$$

With 9 10BaseF users per closet and 12 10BaseF connections per module, the result of one 10BaseF module is entered in region 1A1001's Checklist 3, line 6-E. Region 1A1001's Checklist 3, line 5-E, shows no FDDI users, so a zero is entered in line 6-F. Add the UTP module count for maximum users (line 6-C), the 10BaseF module count (line 6-E), and the FDDI module count (line 6-F) for each communications closet. In region 1A1001, there is a maximum of 7 UTP modules, 1 10BaseF module, and no FDDI modules. The result of 8 modules is entered in region 1A1001's Checklist 3, line 6-G. See example figure 13 for region 1A1001's Checklist 3, lines 5-A through 6-G.

The design team then checks region 3A1001's Checklist 3, line 5-B, and finds 66 maximum users. With the maximum user count per closet of 66, and UTP connections per module of 12, the result of 6 UTP modules is entered in region 3A1001's Checklist 3, line 6-C.

$$\text{6 UTP MODULES} = \text{ROUND UP}\left(\frac{\text{66 USERS}}{\text{12 USERS PER MODULE}}\right)$$

SITE SURVEY CHECKLIST 3
COMMUNICATIONS CLOSET TABLE

5.	User Loads		
	A.	Communications closet region floor area :	2608
	B.	Maximum number users per closet :	75
	C.	Initial user count :	20
	D.	10BaseF connectors :	8
	E.	FDDI connectors :	0
6.	Equipment Loads		
	A.	User cable length needed (feet) :	36,260
	B.	Comm closet to BDF fiber optic cable length :	140
	C.	UTP module count for maximum number of users :	7
	D.	UTP module count for initial users :	2
	E.	10BaseF module count :	1
	F.	FDDI module count :	0
	G.	Maximum I/O module count :	8

EXAMPLE FIGURE 13. Checklist 3 I/O module counts.

Region 3A1001's Checklist 3, line 5-C, shows 15 initial users. Using the same equation as was used for maximum user count, region 3A1001 has 15 initial users and 12 user connections per module. The result of 2 UTP modules for initial users is entered in line 6-D.

$$2\ \mathit{UTP\ MODULES} = \mathit{ROUND\ UP}\ \left(\frac{15\ \mathit{USERS}}{12\ \mathit{USERS\ PER\ MODULE}}\right)$$

Region 3A1001's Checklist 3, line 5-D, shows no 10BaseF users, so a zero is entered in line 6-E. Line 5-E shows no FDDI users, so a zero is entered in line 6-F. In region 3A1001, there are 6 maximum UTP modules and no 10BaseF or FDDI modules. The total maximum number of 6 modules is entered in region 3A1001's Checklist 3, line 6-G. Region 3A1001's Checklist 3 is similar to region 1A1001's and is omitted here for brevity.

Region 2A1001 has previously been designated the BDF, and has no user connections. The BDF Checklist 3, lines 5-A through 5-E, should have zeros to show no user connections. Lines 6-A through 6-Q should show all zeros, since no equipment is needed in the BDF closet to provide user connections. If user connections were provided by the BDF closet, the I/O modules, hubs, local bridges, and patch panels for user connection would be entirely separate from the backbone I/O modules, hubs, and patch panels. This is to prevent BDF users from operating on the building backbone, instead of on their own subnet, like the other users.

Once the three communications closet user module counts have been found, the network totals can be computed. Adding the initial UTP module count from each Checklist 3, line 6-D, gives 2 modules in region 1A1001 and 2 modules in region 3A1001. The total of 4 initial UTP modules is entered in Checklist 5, line 3-A. Summing the line 6-E 10BaseF module count from each Checklist 3 gives a total of 1 10BaseF module, entered in Checklist 5 on line 3-C. No FDDI modules are needed in either closet, so line 3-E receives a zero. See example figure 14 for Checklist 5, lines 3-A through 3-E.

SITE SURVEY CHECKLIST 5
LAN DESIGN WORK SHEET

3. Module Totals for entire LAN project
   - A. Total number of UTP modules needed : 4
   - B. Total number of 10BaseF modules for backbone : ______
   - C. Total number of 10BaseF modules for user connections and Hybrid/FDDI : 1
   - D. Total number of FDDI modules for backbone : ______
   - E. Total number of FDDI modules for user connections : 0

EXAMPLE FIGURE 14. Checklist 5 I/O module totals.

The BDF closet has no LAN user connections, and so no module needs are computed at this time. Region 1A1001 must support eight I/O modules. A small hub will only support four slots and a large hub will support nine. Region 1A1001 needs a single full-sized hub, so a 1 is entered in Checklist 3, line 6-H, and a zero in line 6-I. Region 3A1001 must support 6 I/O modules, and needs a single full-sized hub, as well. Region 3A1001's Checklist 3 has a 1 entered in line 6-H and a zero in line 6-I. For each Checklist 3, the number of hubs is added (lines 6-H and 6-I) to find the number of local bridges needed. In regions 1A1001 and 3A1001, only one local bridge is needed, so a 1 is entered in line 6-J in each Checklist 3. See example figure 15 for region 1A1001 Checklist 3, lines 6-H through 6-J.

SITE SURVEY CHECKLIST 3
COMMUNICATIONS CLOSET TABLE

6. Equipment Loads

H. Number of full-sized hubs needed : 1

I. Number of small hubs needed : 0

J. Number of local bridges needed : 1

EXAMPLE FIGURE 15. Checklist 3 hub counts.

Since the BDF closet has no modules counted yet, no user hub is needed there. The design team will determine later if a BDF backbone hub is needed. Totaling up all the large hubs needed (line 6-H of each Checklist 3) and small hubs needed (line 6-I of each Checklist 3), the design team finds that two large hubs are needed, and no small hubs. A 2 is entered in m 5, line 4-A and a zero in line 4-B. See example figure 16 for Checklist 5, lines 4-A through 4-B.

SITE SURVEY CHECKLIST, FORM 5
LAN DESIGN WORK SHEET

4. **Hub Totals**
   A. **Total number of full-sized hubs :** ________ 2 ________
   B. **Total number of small hubs :** ________ 0 ________

EXAMPLE FIGURE 16. Form 5 hub totals.

For each communications closet, the number of backbone cables needed and the total length of cable must determined. Region 1A1001's Checklist 3, lines 6-H and 6-I, show only one hub to connect to the BDF. Using the backbone cable count equation from stage 5:

$$\begin{array}{c}\textit{BACKBONE CABLE COUNT}\\ \textit{PER COMM CLOSET}\end{array} = \left(\frac{\textit{HUB COUNT} * 8 \textit{ STRANDS PER HUB}}{12 \textit{ STRANDS PER CABLE}}\right)$$

One hub, times 8 strands per hub, divided by 12 strands per cable, resulting in one cable which is entered in Checklist 3, line 6-O.

$$\begin{array}{c}1 \textit{ BACKBONE CABLE}\\ \textit{PER COMM CLOSET}\end{array} = \left(\frac{1 \textit{ HUB} * 8 \textit{ STRANDS PER HUB}}{12 \textit{ STRANDS PER CABLE}}\right)$$

The total backbone cable length needed is the product of Form 31 line 6-B, communications closet to BDF fiber optic cable length, times the line 6-O number of backbone cables needed. For region 1A1001, this is 140 feet times one backbone cable. The result of 140 feet of backbone cable is written into Checklist 3, line 6-P.

$$\begin{array}{c}140 \textit{ FEET OF}\\ \textit{BACKBONE CABLE}\end{array} = \begin{array}{c}140 \textit{ FEET}\\ \textit{PER CABLE}\end{array} * \begin{array}{c}1 \textit{ BACKBONE}\\ \textit{CABLE}\end{array}$$

The BDF Checklist 3, lines 6-H and 6-I, are both zero, so no backbone cable is needed. A zero is entered in lines 6-O and 6-P of the BDF Checklist 3.

The region 3A1001 Checklist 3, lines 6-H and 6-I, also shows one hub, with one backbone cable needed in line 6-O.

$$\frac{\textit{1 BACKBONE CABLE}}{\textit{PER COMM CLOSET}} = \left(\frac{\textit{1 HUB} * \textit{8 STRANDS PER HUB}}{\textit{12 STRANDS PER CABLE}}\right)$$

Line 6-B shows 140 feet per cable, with one cable, for a total of 140 feet of backbone cable entered in region 3A1001's Checklist 3, line 6-P.

$$\frac{\textit{140 FEET OF}}{\textit{BACKBONE CABLE}} = \frac{\textit{140 FEET}}{\textit{PER CABLE}} * \frac{\textit{1 BACKBONE}}{\textit{CABLE}}$$

The region 1A1001 UTP patch panel must support the 75 user drops inside the building and the 9 remote users. This gives a total of 84 cables. Using the UTP patch panel equation from stage 5:

$$\frac{\textit{UTP PATCH}}{\textit{PANEL COUNT}} = \textit{ROUND UP}\left(\frac{2 * \textit{MAX USER COUNT PER CLOSET}}{\textit{UTP CONNECTIONS PER PATCH PANEL}}\right)$$

With a maximum user count of 84, times 2 connections per cable, and 48 user connections per patch panel, the result of 4 UTP patch panels to support all the cables is entered in region 1A1001's Checklist 3, line 6-k.

$$\textit{4 UTP PATCH PANELS} = \textit{ROUND UP}\left(\frac{\textit{84 CABLES} * 2}{\textit{48 CABLES PER PANEL}}\right)$$

The 4 UTP patch panels require 4 times 3.5 inches, or 14 inches of rack space in region 1A1001. The result is written into region 1A1001's Checklist 3 in line 6-L.

14 *INCHES RACK SPACE - 4 PANELS * 3.5 INCHES PER PANEL*

Region 3A1001's Checklist 3, line 5-B shows only 66 maximum users, times 2 connections per cable, for a total of 132 connections. 132 divided by 48 gives 3 UTP patch panels for region 3A1001. The result of 3 UTP patch panels is entered in region 3A1001's Checklist 3, line 6-K.

$$3\ \textit{UTP PATCH PANELS} = \textit{ROUND UP}\left(\frac{66\ \textit{CABLES} * 2}{48\ \textit{CABLES PER PANEL}}\right)$$

The 3 UTP patch panels need 3 times 3.5, or 10.5 inches of rack space in region 3A1001. The UTP patch panel rack space requirement is written into region 3A1001's Checklist 3, line 6-L.

10.5 *INCHES RACK SPACE = 3 PANELS * 3.5 INCHES PER PANEL*

The fiber optic patch panel count can be found using the fiber optic patch panel count equation from stage 5:

$$\begin{matrix}\textit{FIBER OPTIC}\\ \textit{PATCH PANEL COUNT}\end{matrix} = \textit{ROUND UP}\left(\frac{4 * \textit{MAX USER COUNT} + 12 * \textit{HUB COUNT}}{\textit{FIBER OPTIC CONNECTIONS PER PANEL}}\right)$$

The fiber optic patch panel in region 1A1001 must support 84 user cables, with 4 connections per cable, and 12 backbone connections, totaling 348 connections. 348 divided by 96 connections per panel gives 4 fiber optic patch panels. The result of 4 fiber optic patch panels is entered into region 1A1001's Checklist 3, line 6-M.

$$\textit{4 FIBER PATCH PANELS} = \textit{ROUND UP}\ (\frac{\textit{84 CABLES} * 4 + 12}{\textit{96 CABLES PER PANEL}})$$

The 4 fiber optic patch panels require 4 times 7 inches, or 28 inches of rack space in region 1A1001. The rack space required is entered in Checklist 3, line 6-N.

28 INCHES RACK SPACE = 4 PANELS * 7 INCHES PER PANEL

Region 3A1001 needs 66 user cables, with 4 connections per cable, and 12 backbone connections, totaling 276 connections. 276 divided by 96 connections per panel gives 3 fiber optic patch panels. Three fiber optic patch panels is entered in region 3A1001's Checklist 3, line 6-M.

$$\textit{3 FIBER PATCH PANELS} = \textit{ROUND UP}\ (\frac{\textit{66 CABLES} * 4 + 12}{\textit{96 CABLES PER PANEL}})$$

The 3 fiber optic patch panels, times 7 inches per panel, use 21 inches of rack space in region 3A1001. The rack space required is entered in region 3A1001's Checklist 3, line 6-N.

21 INCHES RACK SPACE = 3 PANELS * 7 INCHES PER PANEL

The total rack space in the region 1A1001 communications closet is 14 inches of UTP patch panel (Checklist 3, line 6-L), 28 inches of fiber optic panel (Checklist 3, line 6-N), and 20 inches for the hub (Checklist 3, line 6-H times Checklist 5, line 2-F). This totals 62 inches in closet 1A1001, and is entered in region 1A1001's Checklist 3 in line 6-Q.

$$\begin{array}{c}\textit{62 INCHES}\\ \textit{RACK SPACE}\end{array} = \begin{array}{c}\textit{14 INCHES}\\ \textit{FOR UTP PANELS}\end{array} + \begin{array}{c}\textit{28 INCHES}\\ \textit{FOR FIBER PANELS}\end{array} + \begin{array}{c}\textit{20 INCHES}\\ \textit{FOR HUB}\end{array}$$

If the desired new rack is added to the closet with 72 inches of usable rack space, it will easily hold the 62 inches of new equipment. Enter the 62 inches of rack space needed in line 7-A, and enter 1 on line 7-B for the number of racks needed to provide the space. Checking region 1A1001's Form 3, line 4-C, shows that there is already one usable power circuit, and lines 6-H and 6-I show only one hub needing power, so a zero is entered on line 7-C for additional power needed. Line 4-D shows that the ventilation appeared adequate, and the number of hubs indicated in lines 6-H and 6-I is not excessive, so mark line 7-D for no additional ventilation work needed. Line 4-F shows that a lockable door is already present on communications closet 1A1001, so indicate in line 7-F that no lockable doors need be added. See example figure 17.

SITE SURVEY CHECKLIST 3
COMMUNICATIONS CLOSET TABLE

6. Equipment Loads

K. UTP patch panels needed : 4

L. UTP patch panel rack space needed : 14

M. Fiber optic patch panels needed : 4

N. Fiber optic patch panel rack space needed : 28

O. Number of backbone cables needed : 1

P. Backbone cable needed : 140

Q. Rack space needed : 62

7. Additional Physical and Electrical Requirements

A. Additional rack/cabinet space needed : 62

B. Additional number of racks or cabinets needed : 1

C. Additional 20 amp single load circuits needed : 0

D. Additional HVAC ventilation needed : NO

E. Additional cable routing needs (number, size, location) : NONE

F. Add lockable door or lockable cabinets : NO

EXAMPLE FIGURE 17. Checklist 3 equipment loads and additional requirements.

In region 3A1001, the rack must hold 10.5 inches of UTP panel, 21 inches of fiber optic panel, and 20 inches for the hub. This totals 51.5 inches of rack space in closet 3A1001. The total rack space needed is entered in region 3A1001's Checklist 3, line 6-Q.

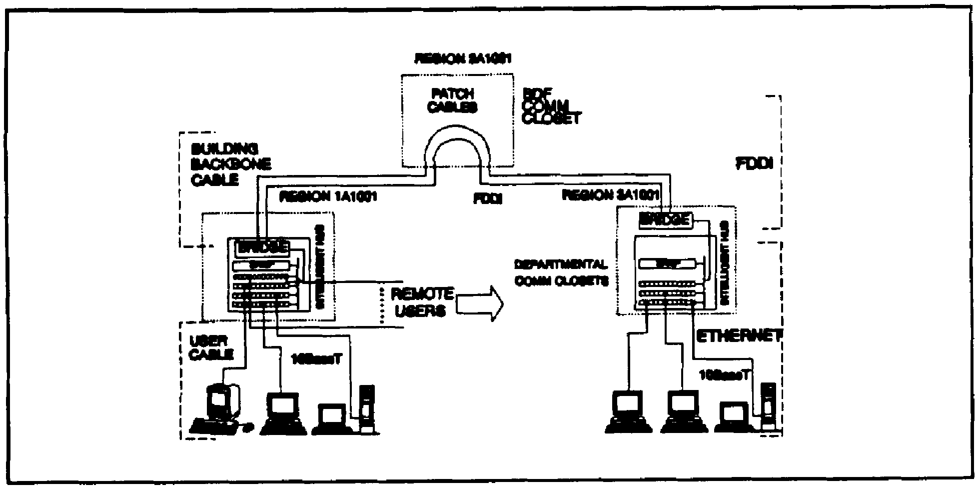
$$\begin{array}{c}\textit{51.5 INCHES}\\ \textit{RACK SPACE}\end{array} = \begin{array}{c}\textit{10.5 INCHES}\\ \textit{FOR UTP PANELS}\end{array} + \begin{array}{c}\textit{21 INCHES}\\ \textit{FOR FIBER PANELS}\end{array} + \begin{array}{c}\textit{20 INCHES}\\ \textit{FOR HUB}\end{array}$$

If a new rack is installed in the communications closet for region 3A1001, it will easily hold all the equipment. Enter the 51.5 inches of rack space needed in line 7-A, and enter one on line 7-B for the number of racks needed to provide the space. Checking region 3A1001's Form 3, line 4-C, shows that there is already one usable power circuit, and lines 6-H and 6-I show only one hub needing power, so a zero is entered on line 7-C for additional power needed. Line 4-D shows that the ventilation appeared adequate and the number of hubs indicated in lines 6-H and 6-I is not excessive, so mark line 7-D for no additional ventilation work needed. Line 4-F shows that a lockable door is already present on communications closet 3A1001, so indicate in line 7-F that no lockable doors need be added. The region 3A1001 Form 3 is similar to the region 1A1001 Checklist 3, and is not shown here for brevity.

For this design, the design team has been directed by the LAN requestor to design an Ethernet LAN with an FDDI building backbone. Since the Multiport Bridging design will not be used, a zero is entered on Checklist 5, line 4-C, for the multiport bridging hub count. See example figure 18 for the network backbone configuration.

Adding up all the local bridges needed (line 6-J of each Checklist 3), the design team finds a total of two local bridges needed, and the result is written into the BDF Checklist 3 in line 8-A. FDDI-to-Ethernet bridging modules will be used in region 1A1001 and 3A1001 communications closets. The 10BaseF module count for the BDF is then zero, which is entered in the BDF Checklist 3, line B-B and

Checklist 5, line 3-B. Since Checklist IA, lines 4-A through 4-C, show no outside connections and the two local bridging modules in closets 1A1001 and 3A1001 can connect directly to each other, no FDDI modules are needed in the BDF hub, and a zero is entered in the BDF Checklist 3, line B-C and Checklist 5, line 3-D. See example figure 19.



EXAMPLE FIGURE 18. Example network backbone configuration.

SITE SURVEY CHECKLIST 5
LAN DESIGN WORK SHEET

3. Module Totals for entire LAN project
   - A. Total number of UTP modules needed : 4
   - B. Total number of 10BaseF modules for backbone : 0
   - C. Total number of 10BaseF modules for user connections and Hybrid/FDDI : 1
   - D. Total number of FDDI modules for backbone : 0
   - E. Total number of FDDI modules for user connections : 0

EXAMPLE FIGURE 19. Checklist 5 I/O module totals.

with no BDF backbone modules indicated in line 8-B and 8-C, the design team decides to eliminate the BDF backbone hub, and enters a zero in the BDF Checklist 3, lines 8-D and 8-E. The backbone cables will still be routed to the BDF fiber optic patch panel and be connected to each other with fiber optic patch cables. This backbone cable arrangement will allow adding a BDF hub later for CUITN connection, or adding more communications closets or users to the LAN. See example figure 20.

SITE SURVEY CHECKLIST 5
LAN DESIGN WORK SHEET

4. Hub Totals
   A. Total number of full-sized hubs : 2
   B. Total number of small hubs : 0
   C. Total number of multi-port bridging hubs : 0

EXAMPLE FIGURE 20. Checklist 5 hub totals.

The fiber optic patch panel is then the only equipment needed in the BDF closet, until more hubs are added or a CUITN connection is desired. Totaling all the backbone cables coming from each communications closet (line 6-0 of each Checklist 3), the design team finds two backbone cables being used, and enters a two in the BDF Checklist 3, line 8-F. The number of fiber optic patch panels needed in the BDF can be found with the stage 5 equation:

$$\begin{array}{c}\textit{BDF FIBER OPTIC}\\ \textit{PATCH PANEL COUNT}\end{array} = \textit{ROUND UP}\left(\frac{\textit{BACKBONE CABLE COUNT}*12 + 24}{\textit{PORTS PER PANEL}}\right)$$

The BDF fiber optic patch panel must support 2 backbone cables plus 24 extra ports for post-wide backbone connection with 96 ports per panel. The result of one panel is written into the BDF Checklist 3, line 8-J.

$$\text{1 FIBER OPTIC PATCH PANEL} = \text{ROUND UP}\left(\frac{\text{2 CABLES} * 12 + 24}{\text{96 PORTS PER PANEL}}\right)$$

In the BDF closet, the sum of lines 6-H and 8-E is zero, so there is no rack space needed for large hubs, and a zero is entered in line 8-I. The sum of lines 6-I and 8-D is zero, so there is no rack space for small hubs, and a zero is entered in line 8-H. The single backbone fiber optic patch panel indicated on line 8-G, times the height of each panel found in Form 5, line 2-K, of 7 inches, gives a total backbone fiber optic patch panel height of 7 inches. The 7 inches are entered in the BDF Checklist 3 in line 8-J. The total user and backbone equipment rackmount space required is found by adding lines 6-L, 6-N, 8-H, 8-I, and 8-J. For the example LAN's BDF, this is 0 + 0 + 0 + 0 + 7, for a total of 7 inches of rack space needed in the BDF closet. The result of 7 inches is written back into line 6-Q, replacing the zero entered there initially.

$$\text{7 INCHES RACK SPACE} = \text{0 INCHES LARGE HUBS} + \text{0 INCHES SMALL HUBS} + \text{0 INCHES UTP PATCH PANELS} + \text{0 INCHES FO PATCH PANELS} + \text{7 INCHES BDF PATCH PANELS}$$

If a new rack is installed in the BDF communications closet, it will easily hold all the equipment. Enter the 7 inches of rack space needed in line 7-A, and enter one on line 7-B for the number of racks needed to provide the space. The extra space in the rack can be used for future additions of a backbone or user hub in the BDF or a CUITN connection. Checking the BDF's Form 3, lines 6-H, 6-I, 8-0, and 8-E, shows no hubs needing power, so a zero is entered on line 7-C for additional power needed. Line 4-0 shows that the ventilation appeared adequate so mark line 7-D for no additional ventilation work needed. Line 4-F shows that a lockable door is already present on the BDF communications closet, so indicate in line 7-F that no lockable doors need be added. The BDF Checklist 3 contains mostly zeros, and is not shown here for brevity.

To find the total number of UTP patch panels needed for the new network, sum all the Form 3's line 6-K. This will equal four panels in closet 1A1001 and three in closet 3A1001. The total of seven UTP patch panels is written into Form 5, line 5-A. To find the total number of fiber optic patch panels required, total all Form 3's, line 6-M, and the BDF Form 3, line 8-F. For the example LAN, this is four panels in closet 1A1001, one in the BDF closet, and three in closet 3A1001. The total of eight fiber optic patch panels is entered in Checklist 5, line 5-B.

To find the total length of user cable required, sum all the Checklist 3's, line 6-A. Region 1A1001 requires 17250 feet of user cable, and region 3A1001 requires 15180 feet. The total of 32430 feet of user cable is entered in Checklist 5, line 6-A. The total length of backbone cable is found by adding all Checklist 3's, line 6-P. Region 1A1001 needs 140 feet of backbone cable, and region 3A1001 needs 140 feet. The total of 280 feet is entered in Checklist 5, line 6-B. See example figure 21.

SITE SURVEY CHECKLIST 5
LAN DESIGN WORK SHEET

5. Patch Panel totals
   A. Total number of UTP patch panels : 7
   B. Total number of fiber optic patch panels : 8
6. Cable totals
   A. Total length of user cable needed : 47,610
   B. Total length of backbone cable : 280

EXAMPLE FIGURE 21. Checklist 5 patch panel and cable totals.

Since no application server needs were recorded in the Site Survey Form I B, the design team decides to use a single computer to function as the network server, file server, and print server and to run any applications that may be added. A zero is entered on Checklist 5, lines 7-A, 7-C, 7-0, and

7-E, since the file server will be used to handle all functions. Review of the NOSs available leads to selection of an operating system that meets most GOSIP and user requirements, and will run on an IBM compatible server.

Checklist 4A for each user/workstation indicates that most LAN users did not know how much file space was needed, so an average of 10 MB is used for each. The test site controller work group requested an extra 100 MB for test files. The total file storage needed is then 45 users, times 10 MB per user, plus 100 MB, or 550 MB. The network server and file server descriptions given above show that only one computer is needed to perform both functions. However, as more LAN users are added to the LAN, additional servers will be needed. A one is entered in Checklist 5, line 7-B, for a single file server. Consulting the CCL shows a total cost of $25,000, which is entered in line 7-B. With only one UPS for the server and no electronics in the BDF requiring an UPS, the total UPS count of one is entered in Checklist 5, line 8. The CCL shows a UPS cost of $500, which is entered in Checklist 5, line 8.

Since all 45 of the User Workstation Forms indicated printer usage, the recommended ratio of 10 LAN users per laser printer gives a total of 5 laser printers needed, which is entered in Checklist 5, line 7-E. Consulting the CCL shows a cost of $2,000 per laser printer, for a total cost of $10,000 for laser printers. These costs are entered into line 7-E. No communications server requirements were identified in the site survey, so a zero is entered in line 7-F. With only 45 initial LAN users, the design team decides to combine E-mail services into the main server, so a zero is entered in line 7-G. The server will be placed in communications closet 1A1001, and will be considered for upgrade to an FDDI network interface in the future, if network performance begins to slow.

The LAN design example Site Survey Checklists 3 and 5, with the information described above, are shown in example figures 22 and 23.

SITE SURVEY CHECKLIST 3
COMMUNICATIONS CLOSET TABLE
(Make a copy for each Comm Closet.)

1. Survey Location Data
Name or number of LAN design project : *Example LAN Design*

2. Label or name for communications closet : *1A1001*

3. Location of communications closet
A. Post : *Fort Redrock*

B. Building : *1001*

C. Floor : *First Floor*

D. Approximate location : *Northeast Corner*

E. Date prepared : *08/16/93*

F. Name of preparer : *DOIM*

Telephone number : *555-1000*

4. Current Physical and Electrical Capacities
A. Unused rack/cabinet space (vertical inches) : *0*

B. Potential rack/cabinet space : *72 inches*

C. Number of unused 20 amp power circuits available for LAN use : *1*

D. HVAC : Additional ventilation required? Yes / No *NO*

E. Cable routing capacity (estimated number of additional cables)
Floor : *0*

Ceiling : *90 cables*

Walls : *0*

Cable routing obstructions in closet? Yes / No *NO*

F. Lockable door to communications closet or lockable electronics cabinet? Yes / No *NO*

EXAMPLE FIGURE 22. Stage 5 Checklist 3.

SITE SURVEY CHECKLIST 3
COMMUNICATIONS CLOSET TABLE

5. User Loads
   A. Communications closet region floor area : *2508 square feet*

   B. Maximum number users per closet : *75*

   C. Initial user count : *20*

   D. 10BaseF connectors : *9*

   E. FDDI connectors : *0*

6. Equipment Loads
   A. User cable length needed (feet) : *36,250 feet*

   B. Comm closet to BDF fiber optic cable length : *140 feet*

   C. UTP module count for maximum number of users : *7*

   D. UTP module count for initial users : *2*

   E. 10BaseF module count : *1*

   F. FDDI module count : *0*

   G. Maximum I/O module count : *8*

   H. Number of full-sized hubs needed : *1*

   I. Number of small hubs needed : *0*

   J. Number of local bridges needed : *1*

   K. UTP patch panels needed : *4*

   L. UTP patch panel rack space needed : *14 inches*

   M. Fiber optic patch panels needed : *4*

   N. Fiber optic patch panel rack space needed : *28 inches*

   O. Number of backbone cables needed : *1*

   P. Backbone cable needed : *140 feet*

   Q. Rack space needed : *62 inches*

EXAMPLE FIGURE 22. Stage 5 Checklist 3. - cont.

SITE SURVEY CHECKLIST 3
COMMUNICATIONS CLOSET TABLE

7. Additional Physical and Electrical Requirements
   A. Additional rack/cabinet space needed : ____ *62 inches* ____
   B. Additional number of racks or cabinets needed : ____ *1* ____
   C. Additional 20 amp single load circuits needed : ____ *0* ____
   D. Additional HVAC ventilation needed : ____ *NO* ____
   E. Additional cable routing needs
      (number, size, location) : ____ *NONE* ____
   F. Add lockable door or lockable cabinets : ____ *NO* ____

8. BDF Only
   A. Number of bridges in the building : ________
   B. Number of 10BaseF modules : ________
   C. Number of FDDI modules : ________
   D. Number of small hubs : ________
   E. Number of large hubs : ________
   F. Number of FO patch panels : ________
   G. Rack Space for small hubs : ________
   H. Rack Space for large hubs : ________
   I. FO patch panel space for backbone : ________

EXAMPLE FIGURE 22. Stage 5 Checklist 3. - cont.

SITE SURVEY CHECKLIST 5
LAN DESIGN WORK SHEET

1. **Survey Location Data**
   Name or number of LAN design project : ____ *Example LAN Design* ____

2. **Design Capacities**
   A. UTP connections per module : ____ *12* ____

   B. 10BaseF connections per module : ____ *12* ____

   C. FDDI connections (single attach) per module : ____ *6* ____

   D. I/O modules per full-sized hub : ____ *9* ____

   E. I/O modules per small hub : ____ *4* ____

   F. Rack space needed per full-sized hub : ____ *20* ____

   G. Rack space needed per small hub : ____ *14* ____

   H. UTP patch panel
   connections per panel : ____ *48* ____

   I. Rack space needed per UTP patch panel : ____ *3.5* ____

   J. Fiber optic patch panel
   ST connections per panel : ____ *96* ____

   K. Rack space needed per FO patch panel : ____ *7* ____

   L. Number of ports in multi-port bridging hub : ____ *20* ____

EXAMPLE FIGURE 23. Stage 5 Checklist 5.

SITE SURVEY CHECKLIST 5
LAN DESIGN WORK SHEET

3. Module Totals for entire LAN project
   - A. Total number of UTP modules needed : ____4____
   - B. Total number of 10BaseF modules for backbone : ____0____
   - C. Total number of 10BaseF modules for user connections and Hybrid/FDDI : ____1____
   - D. Total number of FDDI modules for backbone : ____0____
   - E. Total number of FDDI modules for user connections : ____0____
   - F. Total number of 10BaseT (UTP) NICs for initial users : ____35____
   - G. Total number of 10BaseF (FOIRL) NICs for initial users : ____9____
   - H. Total number of FDDI NICs for initial users : ____0____
   - I. Total number of FDDI management/attach modules for Hybrid/FDDI : ____1____
4. Hub Totals
   - A. Total number of full-sized hubs : ____2____
   - B. Total number of small hubs : ____0____
   - C. Total number of multi-port bridging hubs : ____0____
5. Patch Panel totals
   - A. Total number of UTP patch panels : ____7____
   - B. Total number of fiber optic patch panels : ____8____
6. Cable totals
   - A. Total length of user cable needed : ____47,610____
   - B. Total length of backbone cable : ____280____

EXAMPLE FIGURE 23. Stage 5 Checklist 5. - cont.

SITE SURVEY CHECKLIST 5
LAN DESIGN WORK SHEET

7. **Server totals and costs**

A. **Network servers**
Number of network servers needed : ____ *0* ____

Cost per server : ________

Total cost of network server(s): ________

B. **File servers**
Number of file servers needed : ____ *0* ____

Cost per file server : ____ *$25,000* ____

Total cost of file server(s) : ____ *$25,000* ____

C. **Application servers**
Number of compute servers needed : ____ *0* ____

Cost per compute server : ________

Total cost of compute server(s): ________

D. **Database servers**
Number of database servers needed : ____ *0* ____

Cost per database server : ________

Total cost of database server(s): ________

E. **Print servers**
Number of print servers/controllers : ____ *0* ____

Cost per print server/controller : ________

Number of laser printers needed : ____ *5* ____

Cost per laser printer : ____ *$2,000* ____

Total cost of print services : ____ *$10,000* ____

F. **Communications servers**
Number of communications servers needed : ____ *0* ____

Cost per communications server : ________

Total cost of communications server(s) : ________

EXAMPLE FIGURE 23. Stage 5 Checklist 5. - cont.

SITE SURVEY CHECKLIST 5
LAN DESIGN WORK SHEET

G. E-Mail servers
Number of E-mail servers needed : ________ *0* ________

Cost per E-mail server : ________________

Total cost of E-mail servers : ________________

8. Uninterruptible Power Supply (UPS)
Number of UPSs : ________ *1* ________

Cost per UPS : ________ *$500* ________

Total cost of UPSs : ________ *$500* ________

EXAMPLE FIGURE 23. Stage 5 Checklist 5.- cont.

SITE SURVEY CHECKLIST 5
LAN DESIGN WORK SHEET

9. Design Cost Computation

A. Individual Cost totals

UTP module total cost	: ______________
10BaseF module total cost	: ______________
Full-size hub total cost	: ______________
Small-size hub total cost	: ______________
Local bridge module total cost	: ______________
UTP patch panel total cost	: ______________
Fiber optic patch panel total cost	: ______________
User cable total cost	: ______________
Backbone cable total cost	: ______________
Network server total cost	: ______________
File server total cost	: ______________
Applications server total cost	: ______________
Database server total cost	: ______________
Print server total cost	: ______________
Communications server total cost	: ______________
E-mail server total cost	: ______________
UPS total cost	: ______________
UTP NIC total cost	: ______________
10BaseF NIC total cost	: ______________
Material subtotal cost	: ______________
20% first year maintenance cost	: ______________

B.	Basic Ethernet/Ethernet cost	: ______________
C.	Additional Multi-Port Ethernet/Ethernet cost	: ______________
D.	Additional Ethernet/FDDI cost	: ______________
E.	Additional Hybrid/FDDI cost	: ______________

EXAMPLE FIGURE 23. Stage 5 Checklist 5.- cont.

STAGE 6 - COST ESTIMATES OF LAN DESIGNS

GENERAL

This stage of the design process presents a tabular estimate of equipment, maintenance, and labor costs for 11 LAN configurations; several cost trade-off considerations for the LAN design and installation and operation; and a cost estimate for each of the 4 LAN variations developed by the design team in Stage 5. The design team can estimate the cost of the basic LAN design and the additional cost of each performance variation. The cost estimate that will be computed for the LAN design and variations is intended for cost/performance trade-off analysis only.

TABULAR COST ESTIMATE

As an aid to performing and evaluating the results of the cost estimates, a total cost and per node cost, including a typical system configuration with file servers, print servers, labor and engineering costs, and first year maintenance costs, is provided in table 3-2. The table gives estimates for 50, 150, and 1000 user LANs using (A) Basic Ethernet/Ethernet, (B) Multiport Ethernet/Ethernet, (C) Ethernet/FDDl, and (D) Hybrid/FDDl designs. The cost for the 50 user LAN with a multiport Ethernet backbone was not developed because the network is too small to use the multiport bridge and the cost would match the Basic Ethernet/Ethernet.

All cost estimates are based on second quarter of 1993 engineering best estimates. Each estimate includes costs for contract labor and engineering services. Overall installation labor estimates assume that a new building is being constructed and installation procedures are being conducted at the optimal point in building construction. Cable installation labor estimates assume bundled cable (4 fibers and 8 twisted pair) with an average run of 50 meters, dropped ceilings and/or raised floors, and wall boxes in place prior to cable installation.

Equipment installation labor estimates assume racks and power outlets are already in place. Integration and test labor estimates include configuring bridges, hubs, and other equipment; updating plant-in-place drawings; and assisting in the LAN acceptance test process. The decrease in per node cost with the larger LANs is due to the economy of scale in the labor and engineering work. Use of in-house labor and/or engineering can significantly decrease the final cost.

COST TRADE-OFFS

There are several decisions affecting installation and operations costs that must be made during the LAN design. These decisions concern trade-offs between initial costs and ongoing costs, system reliability/availability, and ease of operation and maintenance.

- Use of single vs. dual power supplies in the intelligent hubs. The reliability of modern LAN hub power supplies provides up to hundreds of thousands of hours between failures, but the power supplies will eventually fail. An intelligent LAN hub with a single power supply will fail anytime the power supply fails, but a hub with dual-redundant power supplies will only fail if both power supplies fail at the same time. As the number of hubs in the network increases, the probability of a power supply somewhere failing (and therefore a hub, as well) also increases. Even power supplies with a 500,000 hour mean time between failure (MTBF) will have a unit fail somewhere each year with 60 or more hubs in use. Use of dual-redundant, load sharing power supplies in each hub will increase the initial cost, but will virtually eliminate down time due to failed power supplies, and will allow replacement within a day or two during normal duty hours, instead of requiring 24 hour a day, instant response.

  If the same 60 hubs had two 500,000 hour MTBF power supplies, and a failed unit was replaced within 48 hours, the rate of network failure due to two power supplies failing simultaneously would be once every 100 years. The design team must decide whether the extra cost of a second power supply for each hub is worth the reduced network down time. The extra initial cost may also reduce the need for a 24 hour a day, 7 day a week maintenance staff, which could save money during network operation of the life cycle of the LAN.

- Designing for many installed user drops or only initial users. The LAN design specifies installing enough wall plates, cables, patch panels, and hubs to handle the maximum possible number of users, and only enough modules to handle initial users. The initially unused user cable adds considerably to the initial cost, and only installing cable for initial users could save a lot of money. But experience in both military and commercial networks indicates that users will be added and users will move. Each new user, or new user location, will require that new cable be strung. Incremental addition of cables is typically more expensive per cable than initial installation. There is also the problem of inadequate sizing on cable trays, cable conduits, hub size, patch panel size, and rack size, resulting in expensive replacement of equipment. The design team must decide whether to reduce initial costs or to make moves and adds quick, easy, and inexpensive for the life of the network.

- On-hand spares. Maintaining one or more of each item used in the LAN will increase initial purchase costs. However, the presence of functional spares will greatly decrease network down time when an item fails. On-hand spares can also allow the same level of service with a less expensive maintenance contract, with failed units mailed back to the factory instead of premium service to provide two hour response time on-site-service.

CREATE COST ESTIMATE FOR BASIC LAN DESIGN

Perform the following calculations to fill out the cost estimate for the Basic Ethernet/Ethernet LAN design. This estimate includes only materials and first year maintenance. The cost of engineering, installation, and integration with contract labor can double the cost of the LAN. Use the component counts in Checklist 5, lines 3-A through 8, and the estimated costs per item from the CCL. Record the individual **equipment/maintenance cost estimates In Checklist 5, line 9-A.**

Perform the following calculations:

UTP Module Cost:

- Multiply the number of UTP modules needed (Checklist 5, line 3-A) by the cost of a UTP module (use item cost in CCL); enter the result in UTP module total cost (Checklist 5, line 9-A).

UTP MODULE COST = MODULE COUNT * COST PER MODULE

10BaseF Module Cost:

- Multiply the number of 10BaseF modules (Form 5, line 3-B) by the cost of each module; enter the result in **10BaseF module total cost (Checklist 5, line 9-A).**

10BaseF MODULE COST = MODULE COUNT * COST PER MODULE

Full-Sized Hub Cost:

- Multiply the number of full-sized hubs (Checklist 5, line 4-A) by the cost of a full-sized hub and enter the result in **Full-sized Hub total cost (Checklist 5, line 9-A).**

FULL SIZED HUB COST = HUB COUNT * COST PER FULL SIZED HUB

Small Hub Cost:

- Multiply the number of small hubs (Checklist 5, line 4-B) by the cost of a small hub; enter the result in **<u>Small-size hub total cost (Checklist 5, line 9-A)</u>**. The hub costs include estimates for the power supplies and SNMP management modules.

SMALL HUB COST = SMALL HUB COUNT * COST PER SMALL HUB

Local Bridge Cost:

- Multiply the number of local bridges (sum of Checklist 5, lines 4-A and 4-B) by the cost of a local bridge and enter the result in **<u>Local bridge module total cost (Checklist 5, line 9-A)</u>.**

LOCAL BRIDGE COST = HUB COUNT * COST PER LOCAL BRIDGE

UTP Patch Panel Cost:

- Multiply the number of UTP patch panels (Checklist 5, line 5-A) by the cost per panel; enter the result in **<u>UTP patch panel total cost (Checklist 5, line 9-A)</u>.**

UTP PATCH PANEL COST = PATCH PANEL COUNT * COST PER PANEL

Fiber Optic Patch Panel Cost:

- Multiply the number of fiber optic patch panels (Checklist 5, line 5-B) by the cost of each fiber optic patch panel; enter the result in **<u>Fiber optic patch panel total cost (Checklist 5, line 9-A)</u>.**

FIBER PATCH PANEL COST = PATCH PANEL COUNT * COST PER PANEL

User Cable Cost:

- Multiply the total amount of user cable needed (Checklist 5, line 6-A) by the cost per foot of user cable and enter the result in **User cable total cost (Form 5, line 9-A).**

USER CABLE COST = USER CABLE LENGTH * COST PER FOOT

Backbone Cable Cost:

- Multiply the length of backbone cable needed (Checklist 5, line 6-B) by the cost per foot of backbone cable; enter the result in **Backbone cable total cost (Checklist 5, line 9-A).**

BACKBONE CABLE COST = BACKBONE CABLE LENGTH * COST PER FOOT

Network Server Cost:

- Enter the total cost of network servers needed (Checklist 5, line 7-A) in **Network server total cost (Checklist 5, line 9-A).**

File Server Cost:

- Enter the total cost of file servers needed (Checklist 5, line 7-B) in **File server total cost (Checklist 5, line 9-A).**

Applications Server Cost:

- Enter the total cost of applications servers needed (Checklist 5, line 7-C) in **Applications server total cost (Checklist 5, line 9-A)**.

Database Server Cost:

- Enter the total cost of database servers needed (Checklist 5, line 7-D) in **Database server total cost (Checklist 5, line 9-A)**.

Print Server Cost:

- Enter the total cost of print servers needed (Checklist 5, line 7-E) in **Print server total cost (Checklist 5, line 9-A).**

Communications Server Cost:

- Enter the total cost of communications servers needed (Checklist 5, line 7-F) in **Communications server total cost (Checklist 5, line 9-A)**.

E-mail Server Cost:

- Enter the total cost of E-mail servers needed (Checklist 5, line 7-G) in **E-mail server total cost (Checklist 5, line 9-A).**

UPS Cost:

- Multiply the number of UPSs needed (Checklist 5, line 8) by the cost per UPS; enter the result in **UPS total cost (Checklist 5, line 9-A).**

UPS COST = UPS COUNT * COST PER UPS

Network Interface Card Cost:

- Multiply the number of 10BaseT (UTP) NICs required (Checklist 5, line 3-F) by the cost of each card; enter the result in **UTP NIC total cost (Checklist 5, line 9-A).**

10BaseT NIC COST = 10BaseT NIC COUNT * COST PER CARD

- Multiply the number of 10BaseF NICs required (Checklist 5, line 3-G) by the cost of each card; enter the result in **10BaseF NIC total cost (Checklist 5, line 9-A).**

10BaseF NIC COST = 10BaseF NIC COUNT * COST PER CARD

First Year Maintenance Cost:

- Total all the costs identified in Checklist 5, line 9. Enter the total in **Material subtotal (Checklist 5, line 9-A).** Take 20 percent of this cost and enter it in **20 % first year maintenance cost (Checklist 5, line 9-A).**

MAINTENANCE COST* = 0.20 * *TOTAL COST OF EQUIPMENT

Basic Ethernet/Ethernet Design Cost Estimate:

- Add the material subtotal (Checklist 5, line 9-A) to the 20 percent first year maintenance cost (Checklist 5, line 9-A) to get the **Basic Ethernet/Ethernet cost (Checklist 5, line 9-B)**.

TOTAL MATERIALS COST = EQUIPMENT COST + MAINTENANCE COST

PERFORMANCE VARIATION COST ESTIMATES

Each of the other performance variations provides increased service, and most variations result in increased LAN equipment costs over the Basic design. The Multiport Bridge variation, which eliminates the need for local bridges in each departmental communications closet, may actually decrease the cost from the Basic Ethernet/Ethernet design. The three other variations will receive incremental cost estimates, the Multiport Bridge and Ethernet/FDDI variations will show a cost above the Basic Ethernet cost, and the Hybrid/FDDI will show an increase over the Ethernet/FDDI cost.

- Multiport Ethernet/Ethernet Variation. Multiply the number of multiport bridging hubs used in the Multiport Ethernet/Ethernet variation (Checklist 5, line 4-C) by the cost of each bridging hub, subtract the total cost of local bridge modules (Checklist 5, line 9-A) and the cost of the BDF backbone hub (BDF Checklist 3 lines 8-D and 8-E times the cost of each hub), and enter the result in **Additional Multiport Ethernet/Ethernet cost (Checklist 5, line 9-C).**

- Ethernet/FDDI Variation. Multiply the number of bridges in the building (Checklist 3, lines 8-A) by the cost of an FDDI-to-Ethernet bridge. Multiply the number of FDDI connection modules for the BDF (Checklist 5, line 3-D) by the cost of each module; add the total cost of FDDI-to-Ethernet bridges (calculated above) to the total cost of FDDI connection modules for the BDF (calculated above), subtract the local bridge module cost (Checklist 5, line 9-A), and enter the result in **Additional Ethernet/FDDI cost (Checklist 5, line 9-0).**

- Hybrid/FDDI Variation. Multiply the total number of FDDI NICs for initial users (Checklist 5, line 3-H) by the cost of each card. Multiply the number of FDDI management/attachment modules needed (Checklist 5, line 3-I) by the cost of each FDDI management/attachment module. Multiply the total number of FDDI modules for user connections (Checklist 5, line 3-E) by the cost of each module. Add the cost of the FDDI NICs, cost of the FDDI management/attachment modules, and cost of the FDDI user connection modules (calculated above) and enter the results in **Additional Hybrid/FDDI cost (Checklist v 5, line 8-E).**

EXAMPLE LAN DESIGN, Continued

CONCLUSION OF EXAMPLE LAN DESIGN

Once the basic design of the Example LAN has been created, the cost estimation is fairly straightforward. The second quarter 1993 CCL, and vendor pricing, where required, give the following item costs:

UTP module cost	=	$1,600.00
10BaseF module cost	=	$3,300.00
Full-sized hub cost	=	$7,000.00
Smell hub cost	=	$4,500.00
User cable cost per foot	=	$1.50
Backbone cable cost per foot	=	$2.30
UTP patch panel cost	=	$230.00
Fiber optic patch panel cost	=	$1,200.00
UPS cost	=	$500.00
Local bridge module cost	=	$5,700.00
Multiport bridge cost	=	$23,000.00
FDDI bridge cost	=	$8,900.00
FDDI network management module	=	$9,400.00
FDDI connection module cost	=	$9,200.00
UTP NIC	=	$300.00
10BaseF NIC	=	$550.00
FDDI NIC	=	$1300.00

Using these item costs, plus the item counts from Checklist 5 lines 3 through 8, the following line item costs are computed and entered in Checklist 5, lines 9-A through 9-E.

The 4 UTP modules needed, times $1,600 each, gives a total of $6,400 for UTP modules.

The single 10BaseF module gives a total of $3,300.

The two full-sized hubs, times $7,000 per hub, gives $14,000 for large hubs.

There are no small hubs used, leaving a zero for this entry.

The two local bridges, times $5,700 per bridges, gives a total of $11,400.

The 7 UTP patch panels, times $230 each, results in $1,610.

The 8 fiber optic patch panels, times $1,200, gives $9,600.

The 47,610 feet of user cable, times $1.50 per foot, results in $71,415 worth of user cable.

The 280 feet of backbone cable, times $2.30 per foot, costs $644.

The only server used initially is estimated at $25,000, and the laser printers at $10,000.

The single UPS for the server will cost $500.

The 35 UTP NICs for initial users, times $300 each, gives $10,500.

The 9 10BaseF NICs, times $550 each, cost $4,950.

Adding all these costs gives a material subtotal of $166,319. Estimating 20 percent of this for the first year maintenance on the equipment adds $33,263. This results in a total cost for the Basic Ethernet/Ethernet design of $199,582, which is just within the tentative budget of $200,000.

The multiport bridging hub adds $23,000, and saves $11,400 in local bridge costs, resulting in an increase in cost of $12,600 over the Basic design.

The Ethernet/FDDl adds 2 FDDI local bridges for a total of $17,800, and saves $11,400 in Ethernet local bridges. The total cost increase over the Basic design is $6,400.

The addition of FDDI users for the Hybrid/FDDI design requires adding two FDDI network management modules, for a total $19,900 over the Ethernet/FDDI design cost. Normally, FDDI user connection modules and FDDI NICs would be added as well, further increasing the cost.

The additional cost of the Multiport Bridging variation could be reduced to a cost savings over the Basic Ethernet/Ethernet design by using a small multiport bridge or router instead of a larger multiport bridging hub. The FDDI backbone only increases the cost slightly since the local bridge prices are similar. The Hybrid design requires FDDI management modules in the hub, and even without interface modules and FDDI NICs, increases the LAN cost. Site Survey Form 5 is shown in example figure 24.

SITE SURVEY CHECKLIST 5
LAN DESIGN WORK SHEET

1. Survey Location Data
Name or number of LAN design project : *Example LAN Design*

2. Design Capacities
   - A. UTP connections per module : *12*
   - B. 10BaseF connections per module : *12*
   - C. FDDI connections (single attach) per module : *6*
   - D. I/O modules per full-sized hub : *9*
   - E. I/O modules per small hub : *4*
   - F. Rack space needed per full-sized hub : *20*
   - G. Rack space needed per small hub : *14*
   - H. UTP patch panel connections per panel : *48*
   - I. Rack space needed per UTP patch panel : *3.5*
   - J. Fiber Optic Patch Panel ST connections per panel : *96*
   - K. Rack space needed per FO patch panel : *7*
   - L. Number of ports in multi-port bridging hub : *20*

EXAMPLE FIGURE 24. Stage 6 Checklist 5.

SITE SURVEY CHECKLIST 5
LAN DESIGN WORK SHEET

3. **Module Totals for entire LAN project**
   - A. Total number of UTP modules needed : *4*
   - B. Total number of 10BaseF modules for backbone : *0*
   - C. Total number of 10BaseF modules for user connections and Hybrid/FDDI : *1*
   - D. Total number of FDDI modules for backbone : *0*
   - E. Total number of FDDI modules for user connections : *0*
   - F. Total number of 10BaseT (UTP) NICs for initial users : *35*
   - G. Total number of 10BaseF (FOIRL) NICs for initial users : *9*
   - H. Total number of FDDI NICs for initial users : *0*
   - I. Total number of FDDI management/attach modules for Hybrid/FDDI : *1*
4. **Hub Totals**
   - A. Total number of full-sized hubs : *2*
   - B. Total number of small hubs : *0*
   - C. Total number of multi-port bridging hubs : *0*
5. **Patch Panel totals**
   - A. Total number of UTP patch panels : *7*
   - B. Total number of fiber optic patch panels : *8*
6. **Cable totals**
   - A. Total length of user cable needed : *47,610*
   - B. Total length of backbone cable : *280*

EXAMPLE FIGURE 24. Stage 6 Checklist 5. - cont.

SITE SURVEY CHECKLIST 5
LAN DESIGN WORK SHEET

7. Server totals and costs

A. Network servers
Number of network servers needed : *0*

Cost per server : ______

Total cost of network server(s): ______

B. File servers
Number of file servers needed : *0*

Cost per file server : *$25,000*

Total cost of file server(s) : *$25,000*

C. Application servers
Number of compute servers needed : *0*

Cost per compute server : ______

Total cost of compute server(s): ______

D. Database servers
Number of database servers needed : *0*

Cost per database server : ______

Total cost of database server(s): ______

E. Print servers
Number of print servers/controllers : *0*

Cost per print server/controller : ______

Number of laser printers needed : *5*

Cost per laser printer : *$2,000*

Total cost of print services : *$10,000*

F. Communications servers
Number of communications servers needed : *0*

Cost per communications server : ______

Total cost of communications server(s) : ______

EXAMPLE FIGURE 24. Stage 6 Checklist 5. - cont.

SITE SURVEY CHECKLIST 5
LAN DESIGN WORK SHEET

G. E-Mail servers
Number of E-mail servers needed : ____0____

Cost per E-mail server : ________

Total cost of E-mail servers : ________

8. Uninterruptible Power Supply (UPS)
Number of UPSs : ____1____

Cost per UPS : ____$500____

Total cost of UPSs : ____$500____

EXAMPLE FIGURE 24. Stage 6 Checklist 5.- cont.

SITE SURVEY CHECKLIST 5
LAN DESIGN WORK SHEET

9. Design Cost Computation

A. Individual Cost totals

UTP module total cost	: $6400
10BaseF module total cost	: $3300
Full-sized hub total cost	: $14,000
Small-sized hub total cost	: 0
Local bridge module total cost	: $11,400
UTP patch panel total cost	: $1610
Fiber optic patch panel total cost	: $9600
User cable total cost	: $71,415
Backbone cable total cost	: $644
Network server total cost	: 0
File server total cost	: $25,000
Applications server total cost	: 0
Database server total cost	: 0
Print server total cost	: $10,000
Communications server total cost	: 0
E-mail server total cost	: 0
UPS total cost	: $500
UTP NIC total cost	: $10,500
10BaseF NIC total cost	: $4950
Material subtotal cost	: $166,319
20% first year maintenance cost	: $33,263

B.	Basic Ethernet/Ethernet cost	: $199,582
C.	Additional Multi-Port Ethernet/Ethernet cost	: $12,600
D.	Additional Ethernet/FDDI cost	: $6,400
E.	Additional Hybrid/FDDI cost	: $19,900

EXAMPLE FIGURE 24. Stage 6 Checklist 5.- cont.

STAGE 7 - CHOOSE LAN DESIGN

GENERAL

During this stage, the LAN design team will select the LAN design and performance variation. The cost estimates in Checklist 5, lines 9-A through 9-D, and the following considerations must be considered in the selection process. Since each site's requirements and budgets are different, this manual does not select a specific LAN design.

LAN DESIGN PERFORMANCE TRADE-OFFS

During the LAN design process, a basic LAN design with three different performance variations has been created. The performance and long-term usability of each variation is discussed below.

Basic Ethernet/ Ethernet LAN

The Basic Ethernet/Ethernet design is ideal for small networks or LAN users who need little more than E-mail access and word processing (office automation). This design provides 10 Mbps shared service among all the LAN users of each communications closet. The Basic Ethernet/Ethernet also limits the building backbone to a total of 10 Mbps for all backbone communication. As LAN usage increases, as LAN users move around, as more applications become LAN based, and as programs and data files become larger, this design will suffer more and more congestion. If the backbone becomes congested, replacing the BDF hub with a multiport bridging hub and using the same cabling will help (upgrade to Multiport Bridging variation). If individual communications closets become congested, segmenting the communications closet into separate work groups will help. Each work group will then either need a separate local bridge and connection to the BDF or a small multiport bridge which must be added to the communications closet to tie all the segments together and to the BDF. Further upgrades, or support of higher data rates, can only occur if the backbone is replaced with an FDDI or similar technology.

Multiport Ethernet/ Ethernet

The Multiport Ethernet/Ethernet variation provides 10 Mbps shared service among all the LAN users of each communications closet and a high composite bandwidth backbone communication between all communications closets, but still only 10 Mbps for any one transfer. This variation virtually eliminates backbone congestion, but limits all data transfers to 10 Mbps or less. If individual communications closets become congested, they can be segmented into separate work groups or subnetworks, with each given a separate connection to the multiport bridging hub. If the LAN grows large enough that the multiport bridging hub runs out of ports, it may be necessary to replace the multiport bridge with an FDDI backbone, using the same cabling (upgrade to the Ethernet/FDDI variation).

Ethernet/FDDI LAN

This variation is good for most office or work group environments where high-speed file transfers are not needed. This variation provides 10 Mbps shared for all the LAN users of a single communications closet, but allows 100 Mbps for the backbone. This should ensure that the backbone does not become congested in the near future, but may still result in congestion in the individual communications closets. The performance of each communications closet can be improved by segmenting into working groups, with separate FDDI bridges for each segment. Individual data transfers that are faster than 10 Mbps still cannot be supported. However, migration to some FDDI user connections (Hybrid/FDDI variation) is simple and does not require replacing any equipment. If the backbone does become congested, a multiport FDDI bridge or router can be used and the communications closets can be divided among several FDDI rings, with each ring connected to the multiport FDDI bridge. with the exception of migration to the Hybrid/FDDI variation, this variation should not require a major upgrade for 5 to 10 years.

Hybrid/FDDI LAN

This variation represents current "state of the art" technology and provides maximum performance. With servers and high data rate LAN users on FDDI connections, the entire LAN will perform better than the Ethernet/Ethernet or Ethernet/FDDI variations. A continued migration of LAN users from Ethernet to FDDI connections can be expected. Backbone congestion can be alleviated by use of the multiport FDDI bridge or router connected to several FDDI rings, with the LAN users divided among the rings.

Future upgrades

All four design variations will allow future upgrade ti asynchronous transfer mode (ATM) or other new technologies without replacing the cabling. Installing multiple UTP and fiber connections for each possible LAN user and terminating them at the wall plates and patch panels should allow use of the LAN with no significant upgrade to the LAN user cabling for 10 to 20 years. The installation of unused fibers in the interconnect cabling should also prevent the need for major upgrade to the cable plant for 10 to 20 years in the cabling between the BDF and communications closet cabling.

FINAL DECISION

You must now consider the pros and cons of each performance variation and make a decision as to which LAN design to use. For a small network (less than 100 users), the Basic Ethernet/Ethernet variation provides adequate performance and low price. For medium sized networks (100 to 200 users), the Multiport Bridging variation provides good performance at a low cost. If the network will eventually migrate to FDDI, the Ethernet/FDDI variation should be used, to avoid making the bridging hub obsolete. For a large network (more than 200 users), the Hybrid/FDDI variation allows FDDI connections to servers. This will provide very high performance for LAN users, even ones with only an Ethernet connection and only costs 15 to 20 percent more than the Basic Ethernet/Ethernet variation. As a final consideration, it is usually wise to build the highest capacity, most reliable LAN affordable. with the rapid growth of LAN usage, what seems like a 20-year solution may require upgrade within 5 years.

SECTION 4. NETWORK START-UP AND OPERATION GUIDELINES

INTRODUCTION

When operating a LAN, certain steps should be taken so that it will run efficiently and with minimum interruption to LAN users. This section provides guidelines to insure smooth operation of the LAN designed in section 3. This section is divided into three parts. The first part provides guidelines for selecting the LAN staff and determining the appropriate composition of that staff. The first part also describes guidelines for both staff and LAN user training. The second part provides guidelines on preparing and installing the hardware and software on a LAN. The last part of this section provides guidelines on the management of a LAN.

PART 1. STAFFING AND TRAINING GUIDELINES

STAFFING

One of the first steps in LAN operation is the establishment of a LAN staff. The number of people and the positions required to support the LAN will vary directly in relation to network size. For a large network, there should be a ratio of two to three LAN staff members for every 100 LAN users. This ratio may increase as LAN size decreases, due to the economy of scale. In any case, it is strongly recommended that a minimum of one senior administrator, one junior administrator, one technician, and one LAN user assistance operator be assigned full-time to support the LAN and LAN user services. As shown in figure 4-1, one senior administrator will supervise a number of junior administrators, technicians, and LAN user assistance operators. Generally, one full-time junior administrator can effectively manage up to 10 LANs (with the appropriate test, measurement, and diagnostic equipment (TMDE)), and one full-time technician can handle up to 100 LAN users and workstations.

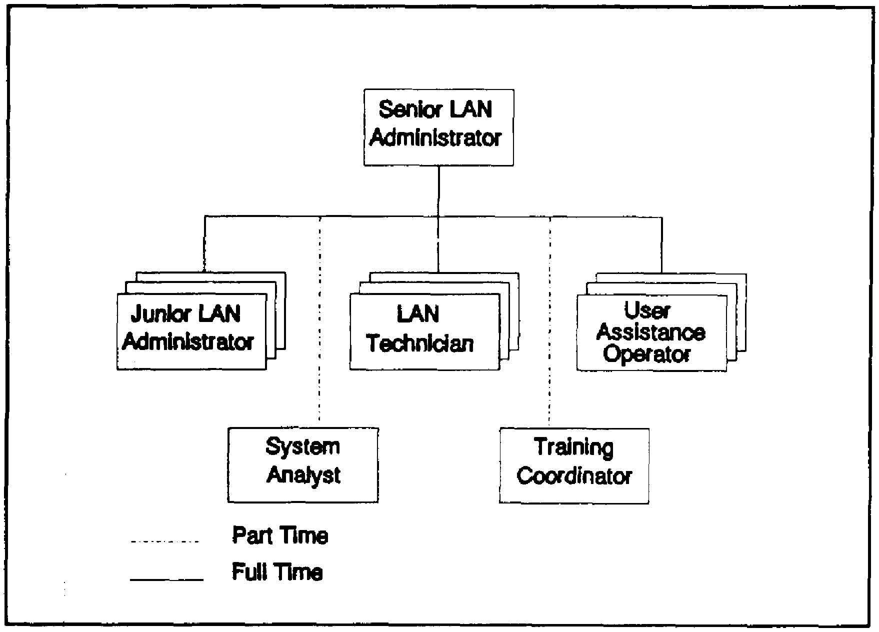


FIGURE 4-1. Sample LAN staff organization.

In addition to these full-time positions, a systems analyst/design engineer and a training coordinator should be assigned for part-time LAN support, depending upon requirements. Personnel for these positions may be drawn from the current staff or from contractor support.

Careful selection of staff should be made using the following guidelines.

Senior LAN administrator

Senior LAN administration duties include supervision of LAN installation and the day-to-day operation of all LAN support functions. This includes supervision of the LAN user assistance branch, which is responsible for managing, monitoring, and resolving information management problems. It is essential that the senior LAN administrator be identified early, to ensure participation in decisions concerning design and configuration of the LAN, management software, and test tools needed to accomplish the task. The senior LAN administrator sets LAN use and operations policies, establishes repair and upgrade procedures, and is the central responsible authority for LAN users in identifying and eliminating LAN viruses.

A critical responsibility of the LAN administrator is to see that file backups occur. All files that are maintained on LAN servers should be backed up on a regular schedule. A minimum schedule should be to backup daily and weekly. In this case, individual files would be needed for each day of the week. On Monday, Tuesday, Wednesday, and Thursday, the procedure should be to backup only modified files (Incremental backup). On each Friday, a full system backup should be performed. The full system backup files should be archived to provide the capability to restore data that might be lost by a catastrophic failure. Archived files should be identified with the system name, date, period covered, and the name of the person who actually performed the backup. All daily and weekly backup files should be stored at a separate location for disaster recovery purposes. The length of time that archived files would be retained should be at the discretion of the Director of Information Management (DOIM).

This position requires a thorough knowledge of the appropriate Institute of Electrical and Electronics Engineers (IEEE) standards and a supplemental knowledge of Government Open Systems Interconnection Profile (GOSIP), as these standards apply to LANs. Experience in managing LAN installations and a working knowledge in LAN design, cable plant installation, and LAN integration and management is desired.

The senior LAN administrator should have at least 4 years LAN experience and a degree in computer science, electrical engineering, management information systems, or a related field.

Junior LAN administrator

The junior LAN administrator adds and deletes LAN users on the network; assigns network addresses and file access privileges; installs various LAN components and support application packages; uses management tools to monitor, detect, and report problems; initiates corrective action when necessary; performs scheduled backups; and maintains the resource inventory as equipment is received for the LAN. This position requires the ability to use the available tools to develop trend and historical usage data.

The junior LAN administrator should have at least 2 years LAN experience and a minimum of 2 years formal training in information systems or a related field.

LAN (electronics) technician

The LAN technician is responsible for installing, maintaining, and repairing electrical devices or circuits. The technician will be responsible for installing and maintaining the LAN components including network cards, hubs, bridges, routers, gateways, workstations, cables, connectors, and microcomputers. The LAN technician maintains as-built drawings of floor plans and make changes to include cable and equipment locations.

The LAN technician should have at least 4 years experience in installation of telecommunications and LAN equipment and a minimum of 2 years formal training. Current knowledge of microcomputer devices, peripheral components, test equipment, and LAN procedures is essential.

LAN user assistance operator

The LAN user assistance operator is the focal point for LAN user interaction in terms of network and telecommunications problems. The LAN user assistance branch is open during normal duty hours with the capability to forward calls after duty hours to a centralized location where a determination is made as to the criticality and sensitivity of the problem.

The assistance branch should be staffed with knowledgeable system experts who can assist LAN users in resolving information management problems in the networking, application, and telecommunication arena. The LAN user assistance operator is responsible for logging in and monitoring problems and for generating trouble tickets for the appropriate information management support staff to resolve. Additionally, the LAN user assistance operator is responsible for interfacing and coordinating with the designated contractor (maintenance) for the repair of hardware equipment as required.

The LAN user assistance operator should have at least 2 years experience in LAN installation and applications. A knowledge of the course material presented in a LAN training classes is essential.

Systems analyst/ design engineer

The computer systems analyst/design engineer is responsible for:

1. Analyzing the requirements and selecting the network approach to provide the necessary service(s).

2. Ensuring that system setup and programming meet the configuration requirements of the design.

3. Verifying that the installation of equipment is complete and the equipment is fully functional prior to operational activation and assignment to the system administrator.

4. Modifying any existing networks for additions, changes, and updates.

The systems analyst/design engineer should have a degree in computer science or a related field, 5 years experience in systems design and analysis of LANs, and a thorough knowledge of the appropriate IEEE standards and GOSIP.

Training coordinator

The training coordinator is responsible for developing and conducting ongoing training courses related to the LAN.

The training coordinator should have 3 years training experience and instructional expertise in network operating systems, electronic message systems, communications systems, and microcomputer application software such as word processing, spreadsheets, database, and menus.

TRAINING

Ongoing training should be provided for the LAN staff and the LAN users.

Administrative design engineer

Training should include both theory and practical hands-on instruction tailored to the installed network. Courses should include duties of the LAN administrator; operating system features and parameter settings; LAN components and features; LAN procedures including access, file management, libraries, security methods, and space management; and familiarization with LAN management.

Technician training

Training should include instruction on installing, operating, and maintaining LAN components.

LAN user training

Successful LAN user training lessens the burden on the LAN administrator/user assistance operator during the day-to-day operations. End user training should provide instruction on how to interact with the network operating system, use of the application software, and hardware provided. Since the system should provide a seamless and transparent interface to the network for the LAN user, this training should take only a few hours. It is important that the LAN users are introduced to the features of the network, are run through the menus, and are shown general LAN concepts. Ideally, this training should be presented in a hands-on format. Issues to be covered should include:

1. Login and logoff procedures
2. Directory and access file rights
3. Using menus
4. Operation of personal computers (PC) and printers
5. How to access print queues
6. How to use applications

7. Virus protection

8. How to use the help desk

9. File backup.

PART 2. LAN INSTALLATION GUIDELINES

SITE PREPARATION

Preliminary engineering and site concurrence documentation should be prepared during the initial survey. Preliminary engineering consists of obtaining or developing drawings and collecting information pertinent to the communications closet. The Site Concurrence Memorandum should record the agreements concerning site preparation and other installation support reached with the LAN user during the site survey and through formal and informal correspondence subsequent to the site survey.

CABLE INSTALLATION

For cable installations, the same general philosophy exists for all buildings - **follow the routes established by the telephone installations.**

Whenever installing cable it is important to make sure:

1. There is space for both the present installations and future expansion.

2. Cable installation will meet applicable fire and safety regulations.

3. Once installed, the cable will be readily accessible for easy maintenance.

Installation rules and regulations

Installation of cable can be performed by in-house technical staff or contractor personnel and should be in accordance with FM 11-487-3. For additional information on cable installation techniques, consult the Army Field Manuals 11-486-5 and 11-487-5, -9, -13, -14, -15, -17, -18, and -19, or Air Force Inside Plant Cable Installation Instructions TO 31-10-2, -6, -7,-11, -12, -13, and -16.

The following is a quick checklist for LAN installations.

1. Choose cable routes: floor, ceiling, or walls; and choose cable routing method: zone, conduit, or point-to-point.

2. Complete communications closet preparation. Install or upgrade conduits, cable trays, or raceways from communications closet to cable routes.

3. Install all cables. Terminate each wire and fiber at both ends of every cable in appropriate patch panels or user information drop wall plates.

4. Tag and label all cables in accordance with FM 11-486-5. Each cable should be uniquely identified. Create or update plant-in-place drawings of all cables installed. Create or update a Cable Connection Database to record user signal paths and maintain a record of all moves, adds, and deletes. This database should include all patch panel connections and cable identification tags.

User cable distribution

There are three basic methodologies for installing user cable between the communications closet and users located on the same floor: in the ceiling, along the wall, or under the floor. when selecting the cable route, the designer should weigh safety, flexibility or rearrangement, initial cost, cost of later additions or alterations, access to the communications closet, and general aesthetics. Cable routed under a raised floor or in a drop ceiling may need to be plenum rated, since these areas often contribute to office air flow. User cable should not be in the same cable tray or conduit as electric power wiring.

Ceiling installation

When installing cable in the ceiling, space requirements and safety codes should be considered. If ceilings are used as air return paths for heating and air conditioning, cables should either be enclosed in approved conduit or channel, or be plenum rated cable. Also, the more cables installed in the drop ceiling, the greater the combined weight; unused cable should be removed to reduce excess weight. Care should be taken to properly dress the cables. where many cables will be run together, cable should be installed in cable trays suspended from the roof/ceiling to minimize weight on the drop ceiling.

There are three basic ceiling distribution methodologies:

1. Zone

2. Raceway

3. Poke-through.

Zone

With zone distribution, the room space is divided into zones. The cables are then run in bundles from the wiring closet to the center of the zone. From the center of the zone, cable is fanned out to walls or utility columns.

Raceway

With raceway distribution, large raceways or cable trays (installed like a series of interconnected suspension bridges hung from the roof) bring the cables to the center of the area. Feeder raceways distribute cables to user locations.

Note: Raceways shall be installed in accordance with applicable electric codes.

Poke-through

With poke-through distribution, cable is run in the ceiling of the level beneath the user and then is "poked through" to the user location. This is an inexpensive method but can weaken the floor structure and violate fire and safety codes.

Wall installation in conduit

Wall installation should be done in conduit. This is because installing cables along the walls of passageways exposes the cables to wear and tear of people passing by, and exposes people to any risk from the cables. With conduit distribution, each group of cables is run in a continuous conduit from the wiring closet to the desired outlet. With this method, distribution is difficult and expensive to rearrange but provides a direct connection and complete protection for cables. Wall conduit installation should only be used when the outlet locations are permanent, device densities are low, and flexibility is not required. This technique is also used for cable run along walls. In older buildings that have neither raised floors nor drop ceilings, conduit or enclosed cable trays run along the walls is the most common method of cable installation.

Floor installation

There are two basic floor installation methodologies:

1. Underfloor duct

2. Raised or access floor.

Underfloor ducts

The underfloor ducts are usually installed while a building is undergoing construction. These ducts are covered metal channels very much like heating ducts. This methodology incorporates straight ducts, curved elbow ducts, and junction boxes where ducts intersect at right angles. The junction boxes act as pulling and repairing points and are usually accessible through tiled or carpeted floor. This approach provides convenient cable routing, but is expensive and typically only used when the building is first constructed.

Raised floor

With a raised floor, the floor stands on pedestals, and any section can be removed for access to the cable beneath. Raised floors are easy to install and repair and provide ease in rerouting underfloor cable; however, they are expensive. With the flexibility of raised floor cable routing, cables can either be bundled and routed in zones, or individual cables can be run point-to-point. The bundled, zone cable routing, similar to ceiling zone routing, takes more initial work and cable, but is more organized and easier to maintain than point-to-point. Point-to-point routing is easy to install, but confusing to maintain, with a tendency towards tangling.

Backbone cable distribution

When running backbone cable between the building distribution frame (BDF) closet and communications closets on the same floor, the cable should be routed along the same paths as user cable or telephone cable. Try to route the backbone cable so that it will not be disturbed when additions or repairs are made in the user cabling or telephone cabling. Any fiber optic cable should be routed and installed carefully to prevent stretching or breaking of the fibers. Unlike user cable, which contains both fiber optic strands and twisted-pair copper wire, backbone cable can be routed near electrical power or noise sources, since it contains no copper wire.

For new buildings or major renovations, consider adding a second cable with 12 single-mode fibers beside each backbone cable. These single-mode fibers will be left dark until required by new technologies.

To install the backbone cable between floors, there must be an opening in the floor between the wiring closets on each level. Since plenum rated backbone cable is recommended in this document, the backbone cable can be routed through air ducts, vertical shafts, or crawl spaces. Three common methods are usually employed.

1. Slots or sleeves

2. Conduits

3. Trays.

Slots or sleeves are rectangular openings that enable cable to pass through. These slots should be fire stopped (plugged with fire retardant materials) to prevent them from being a possible fire path. Conduit is either electrical metallic tubing, rigid metal, or rigid polyvinyl chloride (PVC) pipe. Trays are placed in the ceiling to provide a pathway for the cable. The cable should be plenum rated when run in areas that can induce a fire hazard.

When wiring closets are vertically aligned, a means should be provided to pull cable above and in line with the sleeves or slots. When closets are not vertically aligned, a more circuitous route will have to be designed. To meet safety standards, pathways should not be located in elevator shafts, unless appropriate steps are taken to protect the cable.

User Cable Connection Database

A cable connection database should be used to record the cable/cross connect path from each LAN user into the port on the hub that services them and the backbone cabling between communications closets. The database can be organized into three sections: hub port to patch panel pinout connections, patch panel cross connects, and cable run from the communications closet to the user information drops. An optional fourth section, listing related user names to hub port connections, would aid in correlating network sniffer and hub Simple Network Management Protocol (SNMP) data with the LAN user data traffic. Each entry should detail the location of each end of the cable, the unique identifier on the cable tag, and the cable type and length.

The hub to patch panel section would include the name or location of the communications closet, the number of the hub if more than one is present, the number or unique identifier of the input/output *(I/O)* module, the port number on the module, the patch panel to which the patch cord is connected, and the numbers of the connectors or pins to which it is connected.

The patch panel cross connect section should list the name or location of the communications closet, the patch panels involved, the equipment side connectors or pins, the user side connectors or pins, and the unique identifier of the user cable connected to the patch panel.

The user cable section should list the originating communications closet, patch panel, connectors or pins on the patch panel, floor and room number of the information drop, location within the room of the information drop, and name of user currently connected to the information drop.

The optional fourth section, relating user names to hub port connections, would include a list of current LAN users and what hub, I/O module, and port they are currently connected to.

Cable installation testing

All cables should be tested before being used in the LAN. Cable problems found before LAN start-up will save considerable troubleshooting effort after LAN start-up. Minimal testing of unshielded twisted-pair (UTP) cable should include tests for continuity and shorts. Minimal testing of fiber optic cable should measure the optical power loss. Additional testing of UTP cable should include frequency response, pair-to-pair noise immunity, and a time domain reflectometer to detect and locate defects or irregularities. The optical fiber should be tested for modal dispersion and cable flaws.

EQUIPMENT INSTALLATION

The LAN equipment can be installed in the communications closets once the user and backbone cable has been installed and the closets have been prepared according to the Site Concurrence Memorandum (with any additional racks/cabinets installed, dedicated 20 amp power circuit and receptacle(s), adequate chassis grounds, and ventilation). To prevent electrostatic discharge (ESD) damage to any electrical equipment, grounded wrist straps or other approved ESD protection procedures should be used. For a layout of an ideal communications closet in terms of equipment spacing, including an optional uninterruptible power supply (UPS) and an external fiber distributed data interface (FDDI) bridge, see figure 4-2.

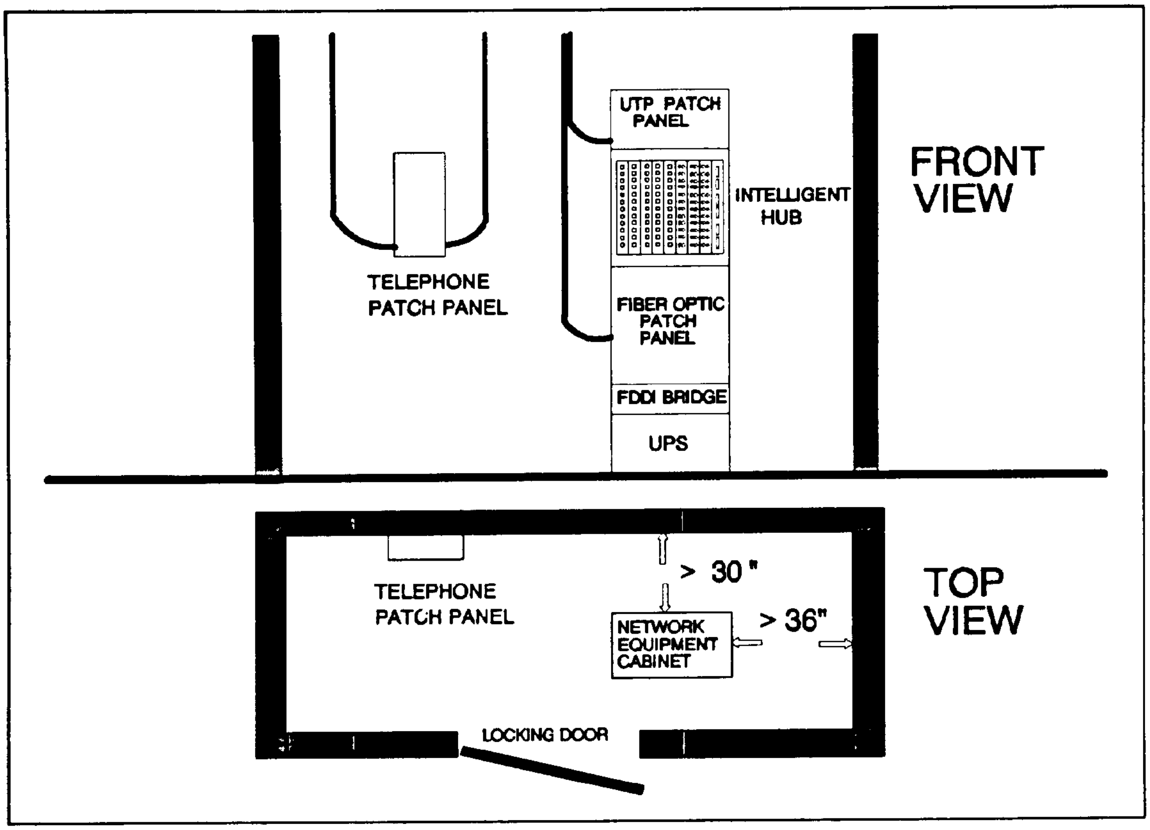


FIGURE 4-2. Ideal communications closet layout.

Communications closet equipment

Equipment installation within the communications closet should first include the assembly of intelligent hubs, patch panels, and any additional equipment such as external bridges, transceivers, and UPSs into LAN racks/cabinets. Placing the fiber optic patch panel above the hub and placing the UTP patch panel below the hub should minimize breakage of fiber patch cables. All user and backbone cables should be routed, bundled, and tie wrapped to prevent flexing and breakage. All power cords should be connected to power strips or should be directly connected to the dedicated LAN power receptacles. If a UPS is used, the LAN equipment should be connected to the power outlet of the UPS, and the UPS should be connected to the LAN power outlet.

The next step should be the installation of assembled hubs and any non-rack mounted equipment. If the hub module placement is not critical for hub backplane interconnection or network segmentation, then similar hub modules should be grouped together in order to simplify cable routing and maintenance.

After hub installation, the backbone fiber optic cable should be connected to the bridging module. If an external fiber to attachment unit interface (AUI) transceiver is required, the transceiver AUI cable should be connected to the bridge AUI port, and the backbone fiber patch cables should be connected to the transceiver fiber ports. If an external FDDI bridge is used, the backbone fibers should be connected to the bridge FDDI ports, and the bridge Ethernet port should be connected to the hub Ethernet backplane through a UTP or AUI port on an interface module. A special AUI cable may be needed. If FDDI user connection modules are used, the backbone FDDI fibers should be looped from the bridge FDDI ports to the hub FDDI module ports and back to the BDF. Figure 4-3 shows the backbone fiber optic connections for a hub with UTP, 10BaseF, and FDDI modules; an FDDI to Ethernet bridge with UTP Ethernet connection; and a BDF fiber optic patch panel.

The manufacturer's instructions should be followed when configuring the switch settings or software settings for the hub, modules, and bridges. The hub and bridge should be self-configuring. All setup settings should be recorded to simplify later maintenance.

Servers

When selecting a location for server installation, the degree of physical access control required by the application should be considered. Prior to the assembly and installation of any server, a parts inventory should be performed to verify that nothing is missing. Attributes such as brand and model of

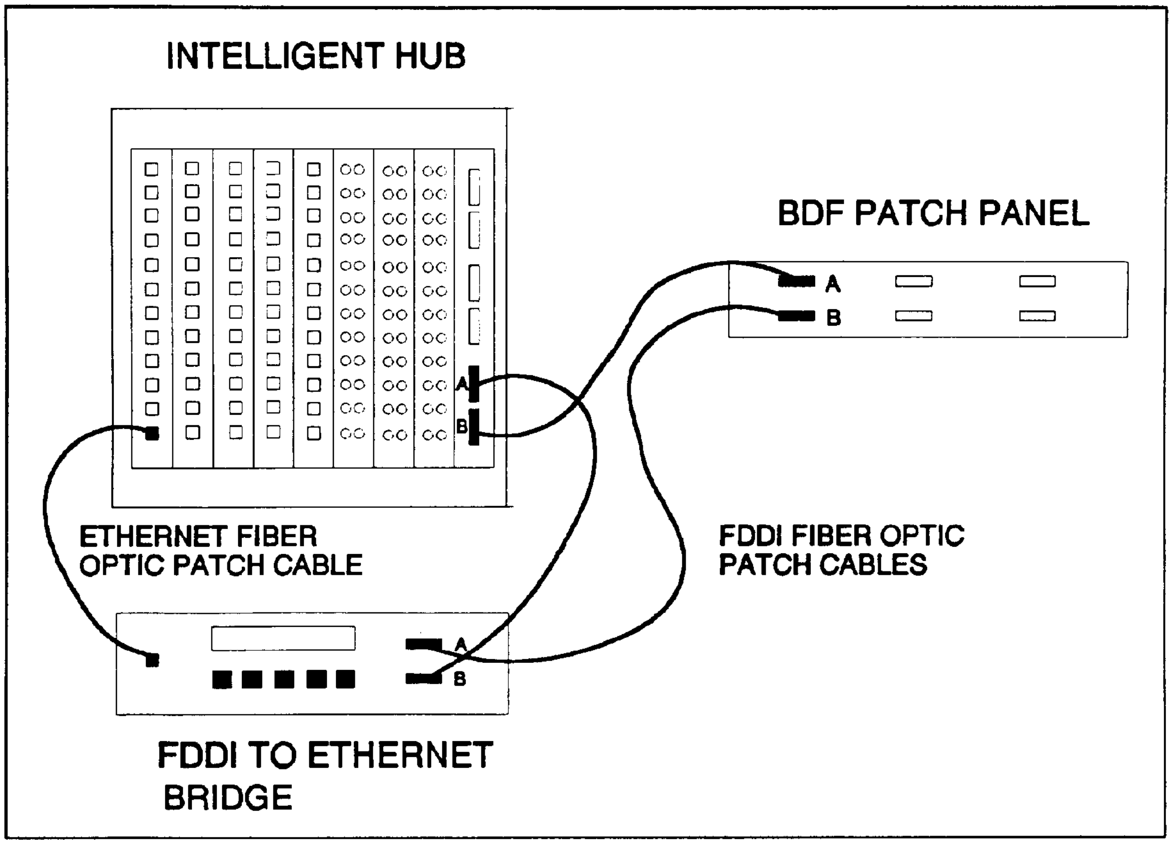


FIGURE 4-3. Possible FDDI backbone connection.

computer, type of hard disk and size, and type and amount of memory should be documented for each server and placed in a file with the inventory. If any warranty cards are included, they should be filled out at this time and returned to the vendor.

During the physical installation process, ESD protection procedures and manufacturer's instructions should be followed. Interrupt and I/O addresses of all cards should be documented. Then the network interface card (NIC) should be installed. If the backup system (tape, compact disk read only memory (CD ROM), and so forth), requires a card, that card should be installed. The power circuit used for the server should be used exclusively for the server. Once the UPS is connected to the receptacle, the UPS functionality should be evaluated according to the manufacturer's directions. After the server is connected to the UPS, the server and UPS should be checked to see that they operate as expected. Once the LAN cable is connected to the server, appropriate test methods should be used as provided by the network operating system (NOS) to validate the server connectivity on the LAN.

Workstations

A NIC is used to convert a standard PC to a network workstation. The NIC is installed into one of the PC bus expansion slots and provides the dedicated connection between the computer and the LAN server. while the mechanics of setting up the NIC are relatively easy, this is best accomplished by the LAN technician. A record of all the various settings for each terminal must be maintained to avoid conflicts in future installations and aid restoration of failed terminals.

SOFTWARE INSTALLATION

Network software must be installed in both the server and workstations that will reside on the LAN to provide proper network operation.

Server NOS installation

Before beginning installation of software, all software required should be on hand (for example, NOS software, LAN drivers, disk drivers, UPS monitoring software). The configuration list of hardware interrupts that was completed when installing the server should then be validated. A virus check should be run on all software before it is installed. Backup copies of the software to be installed should be made and the original disks stored in another location. The backup copies should then be used for installation. A unique name and network number should be selected for each server on the LAN. This may be identified by the LAN administrator as a part of configuration management. If the server is to be on the Internet, the internet protocol (IP) address should be identified. Follow the manufacturer's instructions to load the NOS software. Other communications protocol software should be loaded as desired, for example Transmission Control Protocol/Internetwork Protocol (TCP/IP). If network printers are to be used, software for accessing printers must be installed and configured.

In case the supervisor account is damaged or in-accessible, a secondary supervisor account should be created. A separate password and user identification should be created and assigned supervisor privileges. The LAN administrator, following NOS documentation, should create user accounts for all initial LAN users, including user names, user passwords, file access privileges, and default login scripts.

Workstation network software installation

Following the manufacturer's guidelines and NOS specific instructions, the network driver for the workstation should be created. A backup copy to be used on subsequent workstations should be made. Virus scan software should be installed and run on the workstation to ensure that it is virus free. After installing the driver on a user's workstation, the workstation should be brought up on the LAN and the connection validated. Other communication protocol software, such as TCP/IP, should be loaded.

ACCEPTANCE TESTING

A pre-cutover/post-cutover LAN acceptance test should be conducted in accordance with a government or contractor prepared test plan. Should the test plans be prepared by a contractor, they must be approved by the Government. As a general rule, the acceptance test consists of, but is not limited to, tests which verify the minimal points of functionality to be expected with a newly installed LAN. Each individual test should be a clear derivative of specifications made in the LAN design.

Test plans/procedures should be defined prior to the execution of any tests in a manner prescribed by the Government.

The quality and completeness of testing, the validation of the new LAN, and the accuracy/completeness of the acceptance test should remain with the Government.

Test equipment should be provided by the Government or the contractor. All equipment used should be in calibration and should display the date of the last calibration and next scheduled calibration date. A determination of who shall provide the test engineer and test personnel should be made during the formulation of test plans.

Pre-cutover test

Pre-cutover testing is performed after the installation of LAN hardware/software and prior to cutover. Testing should demonstrate LAN operability, conformance with contract requirements, and LAN readiness for cutover.

Specifically, pre-cutover testing should include:

- Connectivity tests. Connectivity tests verify local and remote, user-to-user/network-to-network LAN connectivity. Such tests examine file transfer, response/acknowledgement time, throughput, etc. Tests shall be performed from NIC-to-NIC/NIC-to-hub (end-to-end) on the LAN. Unused connections and cables installed for future connectivity shall also be tested.

- Intelligent hub/backbone tests. Intelligent hub/backbone tests verify in-system operability of intelligent hubs and other equipment contained in each wiring closet.

- Server tests. Server tests verify server in-system operability. Tests exercise the server’s memory, monitor, connectivity, hard disk (storage), floppy disk, keyboard, backup system/s (i.e., tape drive, CD ROM), network card, parallel card (printer), and UPS. In addition, server tests check file transfer, validate loaded software, and monitor protocols.

- Data transmission quality tests. Data transmission quality tests examine end-to-end data quality and reliability using a line monitor to document bit error rate (BER) and a network sniffer to monitor packet retransmission requests, runts, oversized packets, and garbled packets. Data transmission quality tests check for circuit connectivity and degradation.

- Network stability tests. Network stability tests check network error control and recovery. Tests include disconnecting nodes and powering systems up and down in the middle of network sessions.

- Stress tests. Applicable stress tests (e.g., thermal, power, and load tests) verify LAN functionality outside of standard/normal ranges of operability. Tests shall be incorporated as a function of the LAN requirements outlined in the purchase contract.

- Application tests. Application tests exercise the portion of the LAN software most directly related to the end user. Operation of the LAN application software will also test all elements of the network in normal modes of operation.

- Network management tests. Network management tests exercise the capability of network management software applications and tools installed on the LAN.

Post-cutover test

Post-cutover testing should be performed following the cutover, under actual operating conditions, with live and/or simulated traffic on the LAN for a failure-free period of 30 days. Testing should demonstrate that the typical application load will be supported. Simultaneous testing of infrastructure hardware/software is preferred but not required.

Test reports

At the completion of acceptance testing, a final test report should be developed along with the supporting data collected during testing. Reports should include requirements, test equipment used, results obtained, and any deviation from the original government approved test plan. It is recommended that the test data be copied onto floppy disks. Diskettes should be marked with the source of data, time of collection, and the test scenario involved and should be safely stored to be used as a benchmark for future reference.

PART 3. NETWORK MANAGEMENT GUIDELINES

Effective network management ensures the functionality of the LAN. LAN management tools should be purchased to assist the LAN staff in troubleshooting problems and maintaining a high level of service to the LAN users. These tools should be used by administrative staff to establish a logical map of the LAN during and after installation, as well as to help integrate any existing LANs with the new one. Once the map is complete, these tools can also help determine LAN resource allocation. Integration of network and data center management encourages efficient operation of the network with minimal disruption of services to LAN users.

To comply with the Government Network Management Profile (GNMP) - Federal Information Processing Standard (FIPS) Publication 179 in the area of systems management functions, a LAN implementation must satisfy the requirements as outlined in part 18, clause 8.3.2 of the Open Systems Environment (OSE) Implementors Workshop (OIW) Stable Implementation Agreements (IA), June 1992. In accordance with the GNMP, network management tools must provide for:

1. General management
2. Alarm reporting and state management
3. General event report management
4. General log controls.

5 ELEMENTS OF NETWORK MANAGEMENT

Network management tools in a LAN implementation should incorporate the five elements of the "Network Management for Department of Defense (DoD) Communications," MIL-STD-2045-38000. The five elements are summarized below.

Configuration management

Configuration management is the task of managing and documenting the hardware and software configuration of the LAN. Configurations to be managed include the cabling, equipment, software, NOS user accounts, and file backups. Personnel moves typically affect all of these areas at once. Up-to-date LAN documentation is invaluable for problem resolution, disaster recovery, and capacity planning. However, if discipline is not maintained in promptly updating the LAN documentation after changes occur, the documentation becomes useless. Specific components that should be managed and documented are as follows.

Cable

LAN staff should document the entire cable path, including cable numbers and pair assignments, from each user wall outlet to the LAN or BDF hub, in the Cable Connections Database. This documentation should include the department, name, and phone number of each LAN user to aid in problem resolution. This should be updated after every LAN add, move, or delete, or the database will gradually become useless.

LAN staff should also maintain records in the Cable Connections Database of all interhub and inter-LAN physical linkages such as patch panels, backbone cable pair assignments, and backbone cable locations. The inter-LAN records should also be updated after each inter-LAN cable change.

Equipment

LAN staff should document the inventory of equipment, including component modules. Switch settings, configuration parameters, and disaster recovery procedures should be documented. LAN staff should update the documentation immediately after each equipment move, add, delete, and update.

Software

LAN staff should document the inventory of software packages and component modules, including software installation, configuration parameters, and disaster recovery procedures. The documentation should be updated immediately after each software move, add, delete, and update.

NOS user accounts

LAN staff should document NOS user accounts, rights, and server access. This documentation should include the department, name, and phone number of the LAN users, as well as their node address. LAN staff should update the documentation for each personnel change. Network management-level passwords and security software should be documented. This documentation should be kept separately in a locked or secured room.

File backups

LAN staff should document the file backup procedures described in the LAN staffing section and should keep them updated. As they perform the backups, LAN staff should also update logs showing what was backed up and how the backup media were stored.

Fault management

Fault management is the process of identifying problems, collecting problem reports, tracing problem symptoms, investigating source problem causes, determining effective corrective action, and making repairs or system upgrade suggestions. It is important to discover and correct the underlying causes of network problems.

It is also important to establish policies and set priorities for investigation and repair activities. Will the fault isolation staff operate 24 hours a day, or only during standard duty hours, and with what level of staffing? What level of spares should be kept on hand? The LAN administrator should also set the priorities for investigating problem reports and for effecting expensive repairs or upgrades.

Problem collection and identification

To begin the fault management process, it is first necessary from all possible sources. Three prime sources are the LAN user assistance staff, the network performance management process (described below), and the network technicians. Since the problem may be intermittent or occur only during special circumstances, it is important to get a detailed description of the problem, where on the network it was discovered, and under what circumstances it occurs. Trouble report forms are usually a compromise between the level of detail desired by the fault management people and the level of detail that the LAN users are willing or able to provide. A form that is too complicated might discourage LAN users from reporting all problems.

Symptom identification

Before beginning the fault isolation process, the reported problem symptoms must be investigated and refined. For intermittent problems, the LAN staff should try to re-create the circumstances as closely as possible. If using a network sniffer or protocol analyzer, staff should start as close to the reported source of the problem as possible. Begin reducing the number of conditions needed to produce the symptoms. Staff should try to find the conditions that produce the greatest concentration of defects, checking for line noise or degraded signals on both sides of bridges, routers, hubs and other re-timing or re-transmission devices, and tracing garbled signals back to the location with the poorest signal quality. Staff should look for multiple problems that might be related or due to the same source cause.

Fault isolation

Once the symptoms have been clearly identified and the conditions that produce the error have been found, it is usually easy to determine the fault causing the observed symptoms. When possible, staff should use test equipment to verify the source of the problem. Staff should avoid indiscriminate swapping of cards or modules, or wiggling of cables, connectors, or cards. This will sometimes cause an intermittent failure to disappear for awhile, but the failure often comes back.

Determine source cause

Most network problems can be traced back to a causative agent. The fault manager should find out why the defect occurred in the first place. Then, both the defect and the source cause can be corrected to make sure that this defect does not happen again.

For instance, a LAN user that reports difficulty operating an application is found to be disconnected by the application because the packet timer is timing out. Instead of increasing the packet timer limit, the fault manager should instead find out why the packets are arriving late. The packets may be lost due to an over-loaded bridge, a routing table that sends the packets the long way around, a server with too many applications running at once, or a workstation that is too slow. Some problem causes will be simple and direct, such as failed NICs or broken or defective cables or connectors. However, even these may have source causes that if not fixed will lead to repeat failures later. The NIC may have been damaged by static discharge from people walking on carpeting or by voltage spikes in the ac power. The cable or connectors may be damaged by people walking on them or brushing against them, or by the cable catching on something.

Performance management

The function of performance management is to evaluate long-term behavior of the LAN. Performance management includes collecting and analyzing system statistics, tuning and controlling performance of the LAN based upon such analyses, and generating reports (both realtime and offline).

Accounting management

Accounting management tracks the network resources used by each network user. Standards for traffic data records, billing, bill reconciliation, and service order accounting are being developed within the International Standards Organization (ISO) community. Automatic message detail recording (AMDR) will be required in all switching units, but the format and elements are still in draft stages.

Security management

GNMP has identified five security services as the primary requirements for network management. These services are authentication, access control, confidentiality, integrity, and non-repudiation. GNMP discusses only access control and authentication, but the other three areas are expected to be included in later versions of the standard.

Make note that not all LANs will require all these services. Since the standards are not fully developed, security services are not readily available today. These security services may be provided at one or more of Open Systems Interconnection (OSI) layers 3, 4, and 7.

The network staff should look for the following security services when selecting a network management system (NMS).

Authentication

Authentication services verify the identity of the LAN user and the source of data. LAN subsystems that process BLACK (unclassified) data should have login and password authentication. For example, each LAN user should have a unique login name and password associated with it. The NMS should allow a LAN user three attempts at login. After the third unsuccessful attempt to login, the account would be disabled and the LAN user would be requested to contact the LAN administrator to validate user access.

NOTE: LAN subsystems that process CLASSIFIED or secure data should have security level, login, and password authentication, as well as audit trail and encryption services. The entire LAN has to be system high for the appropriate security level of classified data.

Access control

Access control services allow only access to those areas and resources for which the LAN user has authority. Both discretionary access control (DAC) and mandatory access control (MAC) policies should be used in accordance with DoD 5200.28-STD. These access rules define what data can be received from the LAN and what data can be transmitted over the LAN. Every attempt at data transmission should be verified against the rules before any action takes place. Access control should also be provided for read/write access to files and directories on the servers and hosts. The LAN administrator should be able to control access to network devices such as printers, plotters, and hosts. The NMS should provide access control to login, files, resources, programs, time of day, user, event, terminal identification, routing configuration, inactivity timeout, and time limits.

Data confidentiality

Data confidentiality services protect against unauthorized disclosure. Only those files assigned to a LAN user can be accessed by that LAN user. The implementation of this service is still being developed. It is anticipated that the standard will include ways to ensure that LAN users can be assured of the confidentiality of their files.

Data integrity

Data integrity services protect against unauthorized modification, insertion, or deletion of files (connectionless integrity). The implementation of this service is still being developed. It is anticipated that the standard will include ways that LAN users can be assured files that are sent to other LAN users will be received intact and without alteration of content. The incorporation of virus checking software should assist in the facilitation of this service. All computers and workstations on the LAN should be running virus scanning software.

Non-repudiation

Non-repudiation, with proof of origin, provides the recipient with proof of origin of data and protects against any attempt by the originator to falsely deny sending the data. Non-repudiation, with proof of delivery, provides the sender with proof that a message was sent and/or received. The implementation of this service is still being developed.

APPENDIX A

REFERENCES

STANDARDS

Layer	Standard	Description
Application	ISO 8571	File Transfer, Access, and Management (FTAM)
	ISO 8649 & ISO 8650	Association Control Service Element (ACSE)
	ISO 9072	Remote Operations Service Element (ROSE)
	ISO 10021	Message-Oriented Text Interexchange System (MOTIS)
	ITU-TSS X.400	Message Handling System (MHS) Formerly, this was CCITT X.400
	ISO 9506	Manufacturing Message Specification (MMS)
Presentation	ISO 8822 & ISO 8823	Connection Oriented Presentation
	ISO 8824 & ISO 8825	Abstract Syntax Notation One (ASN.1)
Session	ISO 8326 & ISO 8327	Basic Connection Oriented Session
Transport	ISO 8072 & ISO 8073	Transport Service
Network	ISO 8348	Connection-mode Network Service (CONS)

	ISO 8348/AD1	Connectionless-mode Network Service (CLNS)
	ISO 8208	Packet Level Protocol (PLP)
	ISO 8473	Internetwork Protocol (IP)
	ISO 8878	X.25 to provide CONS
	ISO 8880	OSI Network Service
	ISO 8881	X.25 Packet Level Protocol in LANs
	ISO 9542	ES-IS routing
	ISO 10589	IS-IS routing
Data-link	ISO 4335	High-level Data-link Control (HDLC)
	ISO 7809	High-level Data-link Control (HDLC)
	ISO 7776	X.25 LAPB - compatible DTE Data-link
	ISO 8802-2	LAN logical link control
	ISO 9314-2	FDDI Media Access Control (MAC)
	ANSI X3.T9.5/84-49	FDDI Station Management (SMT)
Physical	ISO 8802-3	Ethernet standards
	EIA RS-232C	Hardware devices
	EIA RS-422	Hardware devices
	EIA RS-423	Hardware devices
	ISO 9314-1	FDDI Physical Layer Protocol (PHY)

ISO 9314-3	FDDI Physical Layer Medium Dependent (PMD)
ANSI X3.T9.5/84-49	FDDI Station Management (SMT)

Federal Standard 1037B, Telecommunications: Glossary of Telecommunications Terms.

EIA/TIA 559, Single-Mode Fiber Optic System Transmission Design Wiring Standard, Electronic Industries Association and Addendum 1.

EIA/TIA 568, Commercial Building Telecommunications Wiring Standard, Electronic Industries Association.

EIA/TIA 569, Commercial Building Standard for Telecommunications Pathways and Spaces, Electronic Industries Association.

NFPA 70-93, NATIONAL ELECTRIC CODE (NEC).

POLICIES

MIL-STD-2045-38000, Network Management for Department of Defense Communications (Draft, subject to changes). This standard requires an installation management entity called a network control center (NCC), subservient to regional/national control centers, that provides local control to all departmental communications systems.

ASQB-SIS-AGL-90-03, Fiber Optics. Existing guidelines for types of cable, distance factors, and number of spares have been determined. Emerging technologies and some of the changes occurring in the vendor offerings may influence these choices but generally will have a minimal impact on the year-old standards.

ASQB-SlS-AGL-91-01, Local Area Networks. This provides architecture guidance to Department of Defense (DoD) engineers, planners, and developers of LANs of Army communications.

ASCG (25-30q), Installation Information Transfer System (IITS) Policy. This technical application provides details and guidelines on implementation of the infrastructure technologies, and network management for information systems on Army installations.

ASQB-SlS-AGL-91-03, Installation Information Transfer System Transition Strategy. This policy requires the Common User Installation Transport Network (CUITN) backbone to meet the transmission needs of all the installation LANS. Duplicate networks cannot be justified where a common network can efficiently and effectively provide service to everyone.

FIPS PUB 146-1, Government Open Systems Interconnection Profile (GOSIP). GOSIP is mandated for all new information transfer systems. The level of compliance is changing as proposed standards complete their review cycle and become a part of the codified umbrella standard. GOSIP is currently being revised and any LAN design should follow the standard in effect at the time of installation.

FIPS PUB 179, Government Network Management Profile (GNMP). This standard became effective 14 June 1993 and is binding 14 December 1994. This standard covers solicitations and contracts for new network management functions and services.

NCSC-TG-005, National Computer Security Center, Red Book, Trusted Network Interpretation.

DoD-5200.28-STD, Department of Defense, Orange Book, Department of Defense Trusted Computer System Evaluation Criteria.

DoD Directive 5200.28, Department of Defense, Security Requirements for Automated Information Systems.

AR-380-1 9, AR-380-1 9-1, AR S380-1, Department of the Army, Information Systems Security.

USAISEC Regulation 34-3, Standardization Engineering Drawings.

NACSIM 5203 (C), National Security Agency Document, TEMPEST Guidelines for Facility,. Design and RED/BLACK Installations (U).

TB 380-41-1, General Information and Guidelines.

AR 530-1 (C), Identification and Applications of Compromising Emanations Control Measures (U).

MIL-STD-188-114A, Electrical Characteristics of Digital Interface Circuits.

MIL-STD-188-124B, Grounding, Bonding and Shielding for Common Long Haul/Tactical Communications Systems, Including Ground Based.

MIL-STD-499A, Engineering Management.

MIL-HDBK-419A, Grounding, Bonding and Shielding for Electronic Equipment and Facilities.

AFTO 31-10-2, Fanning and Forming Conductors for Ground C-E Equipment.

AFTO 31-10-7H, Terminating and Soldering Electrical Connections.

AFTO 31-10-11, Cross-Connections.

AFTO 31-10-12, Metal Ducts and Conduit.

AFTO 31-10-27, Equipment Designation.

USAISEC PAM 34-2, Preparation of Engineering Installation Packages and Standard Engineering Installation Packages.

USAISEC PAM 105-6, Safety Practices and Procedures for Installers.

USAISEC PAM 105-11, Table, Quick Reference for Installers.

DCAC 370-160-2, Site Surveys, Site Selection, and Construction Design Criteria.

DCAC 370-160-3, Installations and Constructions: Site Survey Data Book for Communication Facilities.

NON-GOVERNMENT DOCUMENTS.

National Electrical Code Handbook.

TB - Technical Bulletin.
MIL-STD - Military Standard.
AFTO - Air Force Technical Order.

APPENDIX B

SITE SURVEY CHECKLISTS

SITE SURVEY CHECKLIST, FORM 1A
LAN NEEDS ASSESSMENT

1. Survey Location Data
   - A. Name or number of LAN design project:____
   - B. Name of post:____
   - C. Name or number of building(s):____
   - D. Name or number of floor(s):____
   - E. Date survey performed:____
   - F. Name of LAN requestor:____

     Telephone number:____
   - G. Name of person performing survey:____

     Telephone number:____
2. CAPR or funding for project approved:
3. Estimated user count
4. Out-of-Building connection
   - A. Connection to LAN's in other buildings (Yes/No)

     List other buildings
     :____
     :____
     :____
     :____
   - B. Connection to the DISN gateway (Yes/No):____

     Location of DISN gateway:____
   - C. Connection to post-wide backbone (Yes/No):____

     CUITN connection already in the building (Yes/No):___________________________________

     Location of nearest CUITN attach point:____

SITE SURVEY CHECKLIST, FORM 1 B
SERVERS
(Make a copy for all existing and proposed Servers.)

1. Survey Location Data
   Name or number of LAN design project:____________________

2. Type of Server:

   A. Location of server
      Building name or number:____________________

      Room number:____________________

   B. Number of users:____________________

   C. Type of cable used for connections:____________________

   D. Server description
      Type of computer:____________________

      Memory storage:____________________

      Storage capacity:____________________

      Operating system:____________________

   E. Location of power panel:____________________

   F. Number of direct connect terminals:____________________

   G. Number of remote terminals:____________________

   H. Network applications installed :____________________

      :____________________

      :____________________

      :____________________

3. For communications Servers Only
   A. Number of dial-up lines:____________________

   B. Location of modems:____________________

      Building name or number:____________________

      Room number:____________________

   C. Number of FAX lines:____________________

SITE SURVEY CHECKLIST, FORM 1C
EXISTING NETWORK EQUIPMENT
(Make a copy for each item of existing networking equipment.)

1. Name or number of new LAN design project:____

2. Description of existing LAN that surveyed item of equipment is part of (including spares)

   A. Name of existing LAN or organization supported by existing LAN:___________________

   B. Existing LAN type:____
   (Token ring, Ethernet, Thicknet/10Base5, Thinnet/10Base2, uTP/10BaseT, Fiber/10BaseF, etc.)

   C. Number of workstations connected to existing LAN:_______________________________

   D. Number and type(s) of servers connected to existing LAN ?:________________________

   ____

   E. Will existing servers or workstations be transferred to new LAN ?:__________________

3. Description of piece of networking equipment

   A. Type of equipment (hub, fan-out box, bridge, repeater, etc.):________________________

   description:____

   B. Manufacturer's name:____

   C. Product name (optional):____

   D. Model number:____

   E. Serial number:____

   F. Configuration/options, number and type of ports:__________________________________

   ____

   G. Name or number of building equipment currently installed in:_______________________

   H. Name or number of floor equipment installed in:__________________________________

   I. Approximate location within floor of equipment:___________________________________

   J. Software protocols supported:____
   (Ex. TCP/IP, TP4/CNLP, ISO CNLS(OSI), Novell IPX, Banyan Vines, AppleTalk. DECnet(Phase IV), SDLC, etc.)

   K. Does equipment support SNMP management:______________________________________

   L. Is equipment compatible with and available for use with new LAN:___________________

SITE SURVEY CHECKLIST, FORM 2A
PROJECT DATA
(Make a copy for the LAN Project Manager.)

1. Survey Location Data
   Name or number of LAN design project:____

2. List names or numbers of buildings to be served by this LAN project:

   ____

   ____

   ____

   ____

   ____

   ____

   ____

   ____

   ____

   ____

   ____

   ____

   ____

   ____

   ____

   ____

SITE SURVEY CHECKLIST, FORM 2B
BUILDING FLOOR LOCATION DATA
(Make a copy for each building in LAN project.)

1. Survey Location Data
   Name or number of LAN design project:____

2. Floors to be served by this LAN project
   A. Name or number of building containing these floors:________________________________

   B. List of floors in building to be served by this LAN project:

   ____

   ____

   ____

   ____

   ____

   ____

   ____

   ____

   ____

   ____

   ____

   ____

   ____

   ____

   ____

   ____

SITE SURVEY CHECKLIST, FORM 2C
FLOOR COMM CLOSET LOCATION DATA
(Make a copy for each floor in each building in LAN project.)

1. Survey Location Data
   Name or Number of LAN design project:____

2. List of Communications Closets

   A. Name or number of building containing these comm closets:________________________

   B. Number of floor in building containing these comm closets:_________________________

   C. List of communications closets on this floor

Communications closet name	Approximate location
________________________	____________________________
________________________	____________________________
________________________	____________________________
________________________	____________________________
________________________	____________________________
________________________	____________________________
________________________	____________________________
________________________	____________________________
________________________	____________________________
________________________	____________________________
________________________	____________________________
________________________	____________________________
________________________	____________________________
________________________	____________________________

SITE SURVEY CHECKLIST, FORM 3
COMMUNICATIONS CLOSET TABLE
(Make a copy for each Comm Closet.)

1. Survey Location Data
   Name or number of LAN design project:____

2. Label or name for communications closet:____

3. Location of communications closet
   A. Post:____

   B. Building:____

   C. Floor:____

   D. Approximate location:____

   E. Date prepared:

   F. Name of preparer:____

      Telephone number:____

4. Current Physical and Electrical Capacities
   A. Unused rack/cabinet space (vertical inches):____________________________________

   B. Potential rack/cabinet space:____

   C. Number of unused 20 amp power circuits available for LAN use:____________________

   D. HVAC : Additional ventilation required? Yes / No

   E. Cable routing capacity (estimated number of additional cables)
      Floor:_____________

      Ceiling:___________

      Walls:____________

      Cable routing obstructions in closet? Yes / No

   F. Lockable door to communications closet or lockable electronics cabinet? Yes / No

SITE SURVEY CHECKLIST, FORM 3
COMMUNICATIONS CLOSET TABLE

5. User Loads
   A. Communications closet region floor area:______________________________

   B. Maximum number users per closet:______________________________

   C. Initial user count:______________________________

   D. 10BaseF connectors:______________________________

   E. FDDI connectors:______________________________

6. Equipment Loads
   A. User cable length needed (feet):______________________________

   B. Comm closet to BDF fiber optic cable length:______________________________

   C. UTP module count for maximum number of users:______________________________

   D. UTP module count for initial users:______________________________

   E. 10BaseF module count:______________________________

   F. FDDI module count:______________________________

   G. Maximum I/O module count:______________________________

   H. Number of full-sized hubs needed:______________________________

   I. Number of small hubs needed:______________________________

   J. Number of local bridges needed:______________________________

   K. UTP patch panels needed:______________________________

   L. UTP patch panel rack space needed:______________________________

   M. Fiber optic patch panels needed:______________________________

   N. Fiber optic patch panel rack space needed:______________________________

   O. Number of backbone cables needed:______________________________

   P. Backbone cable needed:______________________________

   Q. Rack space needed:______________________________

SITE SURVEY CHECKLIST, FORM 3
COMMUNICATIONS CLOSET TABLE

7. Additional Physical and Electrical Requirements
   A. Additional rack/cabinet space needed:____

   B. Additional number of racks or cabinets needed:________________________________

   C. Additional 20 amp single load circuits needed:_________________________________

   D. Additional HVAC ventilation needed:____

   E. Additional cable routing needs
   (number, size, location);____

   F. Add lockable door or lockable cabinets:_______________________________________

8. BDF Only
   A. Number of bridges in the building

   B. Number of lOBaseF modules:____

   C. Number of FDDI modules:____

   D. Number of small hubs:____

   E. Number of large hubs:____

   F. Number of FO patch panels:____

   G. Rack space for small hubs:____

   H. Rack space for large hubs:____

   I. FO Patch panel rack space for backbone:______________________________________

   J. Total number of building backbone cables:_____________________________________

   K. Total rack space needed:____

   L. Additional rack/cabinet space needed:____

   M. Additional number of racks or cabinets needed:________________________________

SITE SURVEY CHECKLIST, FORM 4A
USER WORKSTATIONS

1. Survey Location Data
   Name or number of LAN design project:______________________________

2. User name and location:______________________________________

3. Network services needed

   A. E-mail services required? Y / N

   B. File server space needed (Megabytes):__________________________

   C. Network printer services needed? Y / N

   D. Network communications services
      Dial-up line required? Y / N

      FAX services required? Y / N

      Direct terminal connection needed? Y / N

   E. Network Applications
      Word processing? Y / N

      Spreadsheet processing? Y / N

      Database processing? Y / N

      Other office automation applications? Y / N

   F. Other Software Applications used

SITE SURVEY CHECKLIST, FORM 4A
USER WORKSTATIONS

4. Workstation type
   - A. IBM PC [ ]
   - B. IBM PC compatible [ ]
   - C. Apple Macintosh [ ]
   - D. Other [ ]
     specify:____

5. Operating System Software
   - A. MSDOS [ ]
     version:________________
   - B. Macintosh OS [ ]
     version:________________
   - C. UNIX [ ]
     POSIX compliant? Yes / No
     version:________________
   - D. Other [ ]
     specify:________________version:______________

6. System configuration
   - A. Main memory (megabytes):____

   - B. Disk storage capacity (megabytes):_______________________________________

   - C. Expansion bus type
     ISA 8 bit [ ]
     ISA l6 bit [ ]
     EISA [ ]
     MCA [ ]
     NuBus [ ]
     Other [ ]
     specify:____

   - D. Number of unused expansion slots:_______________________________________

   - E. Existing Ethernet interface [ ]
     UTP [ ]
     BNC (thinnet) [ ]
     AUI (thicknet) [ ]
     Fiber optic (ST) [ ]
     Other [ ]
     specify:____

   - F. Use 10BaseF NIC? Yes / No

   - G. Use FODI NIC? Yes / No

SITE SURVEY FORM 4B
APPLICATIONS OR DEPARTMENT SYMBOLS

1. Survey Location Data
   Name or number of LAN design project:____

2. Common user program/data requirements, departments, or work groups

Symbol	Application or Department Name
______	______________________________
______	______________________________
______	______________________________
______	______________________________
______	______________________________
______	______________________________
______	______________________________
______	______________________________
______	______________________________
______	______________________________
______	______________________________
______	______________________________
______	______________________________
______	______________________________
______	______________________________
______	______________________________

SITE SURVEY CHECKLIST, FORM 5
LAN DESIGN WORK SHEET

1. Survey Location Data
   Name or number of LAN design project:______________________________

2. Design Capacities
   A. UTP connections per module:______________________________
   B. 10BaseF connections per module:______________________________
   C. FDDI connections (single-attach) per module:______________________________
   D. I/O modules per full-sized hub:______________________________
   E. I/O modules per small hub:______________________________
   F. Rack space needed per full-sized hub:______________________________
   G. Rack space needed per small hub:______________________________
   H. Connections per UTP patch panel:______________________________
   I. Rack space needed per UTP patch panel:______________________________
   J. ST connections per fiber optic patch panel:______________________________
   K. Rack space needed per FO patch panel:______________________________
   L. Number of ports in multiport bridging hub:______________________________

SITE SURVEY CHECKLIST, FORM 5
LAN DESIGN WORK SHEET

3. Module Totals for entire LAN project
   - A. Total number of UTP modules needed:____
   - B. Total number of 1 OBaseF modules for backbone:______________________________
   - C. Total number of 1 OBaseF modules
     for user connections and Hybrid/FDDI:______________________________________
   - D. Total number of FDDI modules for backbone:__________________________________
   - E. Total number of FDDI modules for user connections:____________________________
   - F. Total number of 10BaseT (UTP) NICs for initial users:___________________________
   - G. Total number of 10BaseF (FOIRL) NICs for initial users:_________________________
   - H. Total number of FDDI NICs for initial users:_________________________________
   - I. Total number of FDDI management/attach modules for Hybrid/FDDI:_______________
4. Hub Totals
   - A. Total number of full-sized hubs:____
   - B. Total number of small hubs:____
   - C. Total number of multiport bridging hubs:______________________________________
5. Patch Panel totals
   - A. Total number of UTP patch panels:____
   - B. Total number of fiber optic patch panels:_____________________________________
6. Cable totals
   - A. Total length of user cable needed:____
   - B. Total length of backbone cable:____

SITE SURVEY CHECKLIST, FORM 5
LAN DESIGN WORK SHEET

7. Server totals and costs

A. Network servers

Number of network servers needed:______________________________

Cost per server: ______________________________

Total cost of network server(s):______________________________

B. File servers

Number of file servers needed:______________________________

Cost per file server:______________________________

Total cost of file server(s):______________________________

C. Application servers

Number of compute servers needed:______________________________

Cost per compute server:______________________________

Total cost of compute server(s):______________________________

D. Database servers

Number of database servers needed:______________________________

Cost per database server:______________________________

Total cost of database server(s):______________________________

E. Print servers

Number of print servers/controllers:______________________________

Cost per print server/controller:______________________________

Number of laser printers needed:______________________________

Cost per laser printer:______________________________

Total cost of print services:______________________________

F. Communications servers

Number of communications servers needed:______________________________

Cost per communications server:______________________________

Total cost of communications server(s):______________________________

SITE SURVEY CHECKLIST, FORM 5
LAN DESIGN WORK SHEET

G. E-Mail servers
Number of E-mail servers needed:____________________________________

Cost per E-mail server:____

Total cost of E-mail servers:______________________________________

8. Uninterruptible Power Supply (UPS)
Number of UPSs:____

Cost per UPS:____

Total cost of UPSs:____

9. Design Cost Computation
A. Individual cost totals

UTP module total cost :____________

10BaseF module total cost :____________

Full-sized hub total cost :____________

Small-sized hub total cost :____________

Local bridge module total cost :____________

UTP patch panel total cost :____________

Fiber optic patch panel total cost :____________

User cable total cost :____________

Backbone cable total cost :____________

Network server total cost :____________

File server total cost :____________

Applications server total cost :____________

Database server total cost :____________

Print server total cost :____________

Communications server total cost :____________

E-mail server total cost :____________

UPS total cost :____________

UTP NIC total cost :____________

SITE SURVEY CHECKLIST FORM 5
LAN DESIGN WORK SHEET

	10BaseF NIC total cost	:_______________
	Material subtotal cost	:_______________
	20% first year maintenance cost	:_______________
B.	Basic Ethernet/Ethernet cost	:_______________
C.	Additional Multiport Ethernet/Ethernet cost:	:_______________
D.	Additional Ethernet/FDDI cost	:_______________
E.	Additional Hybrid/FDDI cost	:_______________

GLOSSARY

TERM	DEFINITION
application server	A centralized computer on a LAN that provides application software for the network.
backbone	The major transmission path for a packet data network (PDN). It is the high-density connectivity portion of any communications network.
bandwidth	The difference between the limiting frequencies of a continuous frequency band.
BNC	A bayonet-locking connector for miniature coax; BNC is an acronym for bayonet-Neill-Concelman. It is used for RG-58 or RG-59 sizes of coax.
bridge	Devices that connect LANs at the data-link layer of the Open Systems Interconnection (OSI) model. Major function is to forward and filter packets, depending upon their destination addresses. A device that connects different LANs so a node on one LAN can communicate with a node on another LAN.
broadcast	1. Transmission of a message intended for general reception rather than for a specific station. 2. In LAN technology, a transmission method carrier sense multiple access/collision detect (CSMA/CD) used in bus topology networks that sends all messages to all stations even though the messages are addressed to specific stations.
brouter	A device with the combined capabilities of a bridge with data handling functions of a router. Typically, a brouter will route one protocol, such as internet protocol (IP), and bridge all other traffic. Generally it is used when there is a mix of homogenous LAN segments with two very different segments.

TERM	DEFINITION
bus	One or more conductors or optical fibers that serve as a common connection for a related group of devices.
cable conduit	A pipe or tube used to protect one or more cables going from one place to another.
cable tray	An open-top channel used to support and route cables.
circuit switched	This connection is similar to standard voice lines. The communication path is fixed for the duration of the connection. The sending computer would initiate a call via a modem to the receiving computer, transfer the data, and then terminate the link. This is a dedicated circuit for the entire session.
client-server	In a communications network, the client is the requesting machine and the server is the supplying machine.
closed system	A network which does not interoperate with networks of a different vendor. It is a vendor proprietary system.
coax	“CO-AXial,” a type of cable with a conductive coating (foil or braid) surrounding an insulated center conductor. It is used to carry high-frequency signals.
collapsed backbone	The backplane in a hub which contains the backbone bus for the input/output (I/O) modules of the hub.
communications closet	An enclosure where communication interconnect patch panels and networking connection equipment are located.
communicating devices	A device used in the electronic connection of a network.

TERM	DEFINITION
communications server	A computer that controls one or more modems or terminals, provides protocol conversion, or acts as a gateway to other networks.
concatenate	The connection or linking of a series.
connectionless	A service in which data is presented, complete with a destination address, and the network delivers it on a best effort basis, independent of other data being exchanged between the same pair of LAN users.
connection-oriented	A service in which a connection-setup procedure must be implemented before data can be exchanged between two LAN users. This often includes ensuring that data packets will be delivered in order, without loss or duplication. If a minimum level of service cannot be maintained, the connection is automatically terminated.
database server	The database operations are performed on a centralized server. Where databases are stored on the LAN.
dc resistance	The resistance of a circuit with no alternating current (ac) components. Resistance to an unchanging current, no reactance.
de facto	The exercising of power as if legally constituted. Standardized by way of widespread use.
dielectric	Any substance in which an electric field may be maintained with zero of near-zero power dissipation; a nonconductive material.
directory	Directories represent the path established to store and retrieve the actual files off the storage media.

TERM	DEFINITION
distributed processing	An arrangement that allows separate computers to share work on the same application program. In a distributed processing system, a program executes tasks on many processors spread around the network.
E-mail, Electronic mail	Electronic Mail refers to messages sent between subscribers electronically via a public or private data communications system. LAN users can send mail to a single recipient or broadcast it to multiple users on the system.
E-mail server	A computer that receives stores, and forwards electronic mail, either to other E-mail servers or to the LAN user.
EIA/TIA	Electronics Industries Association/ Telecommunications Industry Association. USA trade organizations that issue standards and contribute to the American National Standards Institute.
engineering drawing	The floor plans of buildings drawn to scale and showing details of internal structures, such as walls and doorways.
Ethernet	A de facto standard, developed first by Xerox and then sponsored by Xerox, Intel, and DEC. An Ethernet LAN can use twisted-pair (TP), fiber optic, or coaxial cables. Ethernet is used to designate Institute of Electrical and Electronics Engineers (IEEE) 802.3 compliant networks.
expansion bus	The portion of the computer design for adding capabilities, such as the printer controller, disk controller, or network interface card.

TERM	DEFINITION
fax server	A dedicated communication personal computer (PC) for providing the network with the ability to share incoming and outgoing facsimile transmissions.
fiber optics	A fiber optic cable consists of a strand of fiber material, usually glass, inside of a protective jacket. Signals are transmitted in the form of light pulses.
file server	The file server is the central node that provides network services found in the network operating system. The server which provides bulk storage of user files.
gateway	Often the gateway changes the format of the messages to conform to the applications program at the receiving end. This allows networks with totally incompatible protocols to communicate.
hardware	Equipment (as opposed to a computer software) such as mechanical, electrical, magnetic, or electronic devices.
high-speed router	A device that sorts packets of information on a network and forwards to the correct network. Routers can translate between a wide variety of cable and signaling schemes.
hub	The hardware equipment used at the center of a star topology network or cabling system. The hub can be active or passive. An active hub serves as a repeater to other LANs and will amplify as well as recondition the signal. A passive hub provides no amplification and contains no intelligence like the active hub.
hybrid cable	A cable containing more than one type of medium, typically, unshielded twisted-pair (UTP) and fiber optic.

TERM	DEFINITION
index of refraction	The ratio of the velocity of light in free space to the velocity of light in a given material.
information drop	A wall or floor plate where users connect telephone or network equipment to the building's communications infrastructure.
intelligent hub	The hardware equipment used at the center of a star topology network or cabling system with inherent remote management capabilities.
interconnection	The linking together of interoperable systems.
internetwork	A set of interconnected, logically independent networks. The constituent networks are usually administrated separately and may be composed of different transmission media.
interoperable	The ability of software and hardware on multiple machines from multiple vendors to communicate meaningfully.
intranetwork	Within the boundaries of a local network.
jabber packet	An over length Ethernet packet (greater than 1518 bytes long).
Kevlar	A fibrous material of very high strength.
local bridge	The local bridge directly connects two LAN cable segments. Bridges use tables to decide whether to pass or hold data messages (similar to routers).
login	The procedure which allows the user access to a server on a LAN.
logoff	This procedure terminates connection with a particular server.

TERM	DEFINITION
mainframe computer	A large-scale computer, normally supplied with peripherals and software from a single vendor, commonly a closed architecture. Also called host or central processing unit (CPU) or mainframe computer.
media	This refers to the method of transmission, such as infrared (IR), microwave, or the type of cable (coaxial, UTP, or fiber optic).
media access control (MAC)	Bottom sublayer of OSI data-link layer (layer 2). It represents the physical station address or the hardware address of the network board. A MAC address is unique for every station. Bridges rely on MAC addresses for operation.
message switching	A routing technique using a message store-and-forward system. No dedicated path is established. Rather, each message contains a destination address and is passed from source to destination through intermediate nodes. At each node, the entire message is received, stored briefly, and then passed on to the destination node.
micron	One-millionth of a meter.
microprocessor	A computer-on-a-chip or the CPU. This component determines and controls the computer's processing characteristics, power, and types of software programs it can process.
minicomputer	A small-scale of medium-scale computer, usually operated with interactive dumb terminals and often having an open architecture. Also called mini for short.

TERM	DEFINITION
modal dispersion	Dispersion resulting from the different transit lengths of different propagating modes in a multimode optical fiber.
modem	A contraction of the terms modulator and demodulator. It modulates computer signals from digital-to-analog, analog-to-digital, and digital-to-digital form, thus enabling data to travel over a telephone system.
mouse	A hand-held computer input device that generates the coordinates of a position indicator which appears on a computer monitor, and operates by being moved.
M-port	A single-attach connection at an fiber distributed data interface (FDDI) concentrator.
multimode fiber	A fiber optic cable wide enough to allow light to reflect internally at several different angles. Multimode can use a mix of light frequencies.
multiport bridge	A bridging device that connects more than two adjacent networks. Multiport bridges with a high internal bandwidth can simultaneously support full-speed communication on all ports.
network operating system	A program that manages resources across an entire LAN, such as remote file systems that are accessible by other workstations, the loading and execution of shared application programs, and I/O to shared network devices.
node	Any device connected to a network, such as a workstation or file server.

TERM	DEFINITION
open system	Interoperability solution in which a vendor makes products compliant with universally accepted standards. The development of the OSI model is a step towards standardization.
operating system	Software used to control the basic operation of a computer. It allows users to access files, run programs, use printers, etc.
packet switch connection	This connection provides a shared physical connection. A message is submitted to the network for delivery. The message is subdivided into specific size packets for transmission. This type of connection is not time sensitive. A virtual circuit which defines the logical connection is created.
peer-to-peer	A LAN that allows all LAN users to access data on other workstations.
peripheral device	Any equipment, distinct from the central processing unit, used to provide additional capabilities or process data for entry into or extraction from a computer.
peripherals	See peripheral device.
plenum	An open space, used for office air circulation, where cable can be run. Due to fire and noxious gas potentials, special safety cable must be used.
plenum rated cable	A cable that has a special coating or sheath which minimizes the release of noxious gases when exposed to flames or heat.
point-to-point link	Transmission of data between a single sender and receiver. A point-to-point link is a circuit connecting two stations to each other only, with no intermediary node.

TERM	DEFINITION
print server	The print server software accepts jobs from application programs running on client stations, stores them on a hard disk, and sends them to a printer when the job's turn occurs in the queue. Typically, the print server is in the file server however, it may be on any PC on the LAN.
protocol	In communications, a set of rules and regulations that govern transmitting and receiving of data. The means used to control the orderly exchange of information between stations on a data-link or on a data communications network or system, Also called line discipline.
random access memory	RAM, the working memory of the computer in which application programs and data can be stored and used by the CPU.
read only memory	ROM, an integrated circuit used for storing frequently used computer instructions and data. ROM is permanent memory because data is not erased when the power is turned off.
relay rack	A structure with standard mounting rails of 19.5 inches wide. It is used to mount electronic equipment.
remote access	The connection between a computer or terminal to any network service, over either a LAN, dial-up modem, or other communications technique.
remote bridge	Remote bridges operate in pairs, connecting the LAN cable segments using an intermediary inter-LAN link such as a leased telephone line.

TERM	DEFINITION
repeater	A device used to extend transmission ranges/distances by restoring signals to their original size or shape. Repeaters function at the physical layer of the OSI mode.
RG-58 A/U	Coaxial cable assembly used as "Ethernet" thinnet 50 ohm cable.
ring	A network in which every node has exactly two branches connected to it. The nodes are connected in series.
RJ-45	A modular connector with eight contacts, typically used in network connections of UTP cabling.
router	Devices that function at the network layer of the OSI model and are protocol specific. Routers direct packets generated between networks, thereby reducing network traffic.
routing table	Routing tables are used to determine the best path to send packets. Routers examine the source and destination addresses in the packet to determine where the packet came from and where it needs to be delivered. Cost and distance are also used in routing determination.
RS-232-C/D	A physical interface protocol (EIA RS-232-C/D), the mechanical interface is the 25-pin ISO 2110 connector. It is used for the interface between data terminal equipment and data communications equipment.

TERM	DEFINITION
RS-449	A physical interface protocol, EIA RS-449 was developed to attain improved performance over EIA RS-232-C. It enables longer cable distance, higher maximum data rates, and additional interface functions, for example, maintenance loopback testing. The interface was designed to be interoperable with RS-232 equipment. It uses a general purpose 37-pin connector (ISO 4902) for the basic interface and a separate 9-pin connector if a "secondary channel" operation is in use.
server	A high-speed computer in a LAN used to store programs or data files shared by the LAN users on the network or perform network management of the LAN. There are different types of servers (such as file, database, print, fax, and communications), each performing a specific activity for the LAN.
single-mode fiber	A small core diameter fiber which allows a single mode of light; light only travels along the axis of the fiber. It can be used over greater distances than MultiMate fiber.
software	A computer program or set of stored instructions and procedures held in some storage medium, such as read/write memory (RAM) that can be recalled or loaded in the computer for execution.
spread spectrum	Techniques that utilize signal frequency hopping at a rapid rate or that spread a transmitted signal across a range (band) of carrier frequencies.
star	A radial (starlike) configuration of communication-network nodes such that there is a direct path between each node and a central node that serves as a central distribution node.

TERM	DEFINITION
star coupler	A fiber optic coupler in which power at any input port is distributed to all output ports.
system memory	The part of a computer where programs and information are stored while they are being used.
T1	T-carrier designation for a channel rate of 1.544 megabits per second (Mbps).
T3	T-carrier designation for a channel rate of 44.736 Mbps.
tap	In cable-based LANs, a connection to the main transmission medium.
10Base2	A network conforming to the IEEE 802.3 local area network standard. The network is capable of carrying information at rates up to 10 Mbps over distances up to 185 meters (approximately 600 feet) using RG-58 coaxial cable.
10Base5	A network conforming to the IEEE 802.3 local area network standard. The network is capable of carrying information at rates up to 10 Mbps over distances up to 500 meters (approximately 1600 feet) using RG-8 coaxial cable.
10BaseF	The standard defined for Ethernet communication over fiber optic cable.
10BaseT	A network conforming to the IEEE 802.3 local area network standard. The network is capable of carrying information at rates up to 10 Mbps over distances of 100 meters (approximately 325 feet) using twistedpair cable.
terminals	Any device capable of sending or receiving data over a data communications channel.

TERM	DEFINITION
Terminate and Stay Resident	TSR is a unique application program that will stay in the computer's memory even though it is not currently the program being used. It is also called memory resident. Many TSR programs can be instantly entered from another program by the use of a hot key.
thicknet	A type of coaxial cable used for a 10Base5 network. See 10Base5
thinnet	A type of coaxial cable used for a 10Base2 network. See 10Base2.
timesharing	A method of computer operation that allows several interactive terminals to use a computer and its facilities; although the terminals are actually served in sequence, the high-speed of the computer makes it appear as if all terminals were being served simultaneously.
token	That part of a packet used for network access on Token Ring LANs; the station that "owns" the token is the station that controls the transmission medium.
token-passing	An access method in which a special message (token) circulates among the network nodes, giving a node permission to transmit.
token-ring	The token-ring is described as a ring topology because data is passed from station to station until it returns to the starting point. The token-ring usually has a physical star topology.
topology	The architecture of a network, or the way circuits are connected to link the network nodes together.
transceiver	A single device that combines the functions of a transmitter and a receiver.

TERM	DEFINITION
trustee	The user is assigned rights to perform operations, such as read, write, create, and erase files in a directory. The user entrusted with these rights is called a trustee and the actual rights assigned are called trustee assignments.
V.35	International Telecommunication Union - Telecommunication Standardization Section (ITU-TSS) (formerly International Consultative Committee for Telephone and Telegraph (CCITT)) standard for connection and signaling.
watt	A unit of power, defined as the electrical work required to drive a current of 1 ampere across a potential of 1 volt.
workstation	A computer used to run programs and provide communication to the LAN.
X.25	An ITU-TSS protocol for packet switching networks.
ac	alternating current
ACSE	Association Control Service Element
AMDR	automatic message detail recording
AMMUS	Air Force Minicomputer Multi-User System
ANSI	American National Standards Institute
ASN.1	abstract syntax notation one
ATM	asynchronous transfer mode
AU	attachment unit interface
AWG	American Wire Gauge
AWSCEM	Army Wide Small Computer Equipment Maintenance
B-ISDN	Broadband-ISDN
BDF	building distribution frame
BER	bit error rate
BNC	bayonet connector
BOM	bill of materials
BPA	Blanket Purchase Agreement
bps	bits per second
BRI	basic rate interface
CAPR	Information capability request

TERM	DEFINITION
CCITT	formerly International Consultative Committee for Telephone and Telegraph, renamed ITU-TSS
CCL	Certified Components List
CDDI	copper distributed data interface
CD ROM	compact disk read-only memory
CLNS	Connectionless-Mode Network Service
Comm	communication
CONS	Connection-Mode Network Service
CNLP	connectionless network layer protocol
CPU	central processing unit
CSMA/CD	Carrier Sense Multiple Access/Collision Detection
CSU	channel service unit
CUITN	Common Users Installation Transport Network
DAC	discretionary access control
DARPA	Defense Advanced Research Projects Agency
dB	decibel
DCE	data communications equipment
DCID	Director Central Intelligence Directive
DDS	digital data service
DEC	Digital Equipment Corporation
DIAM	Defense Intelligence Agency Manual
DISN	Defense Information Systems Network
DoD	Department of Defense
DOIM	Director of Information Management
DOS	disk operating system
DS1	digital signal 1
DSN	Defense Switched Network
DSU	digital service unit
DTE	data terminal equipment
ECMA	European Computer Manufacturer’s Association
EIA	Electronics Industries Association
EIP	engineering installation plan
EISA	extended industry-standard architecture
EMI	electromagnetic interference
ESD	electrostatic discharge
FCC	Federal Communications Commission
FDDI	fiber distributed data interface
FIPS	Federal Information Processing Standard

TERM	DEFINITION
FO	fiber optic
FOIRL	Fiber Optic Inter-Repeater Link
FTAM	File Transfer, Access, and Management
Gbps	gigabits per second
GHz	gigahertz
GNMP	Government Network Management Profile
GOSIP	Government Open Systems Interconnection Profile
GUI	graphical user interface
HDLC	High-Level Data-Link Control
HP	Hewlett Packard
HVAC	heating, ventilation and air conditioning
IA	Implementation Agreement
IBM	International Business Machines Corporation
IDF	intermediate distribution frame
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IITS	Installation Information Transfer System
INIC	intelligent network interface card
I/O	input/output
IP	Internetwork Protocol
IPX	internetwork protocol exchange
IR	infrared
IRQ	interrupt request
ISDN	Integrated Services Digital Network
ISM	industrial, scientific, and medical
ISO	International Standards Organization
ITU-TSS	International Telecommunication Union - Telecommunication Standardization Sector
kbps	kilobits per second
khz km	kilohertz kilometer
LAN	local area network
LED	light emitting diode
LLC	logical link control
MAC	mandatory access control
MAC	media access control
MAU	medium attachment unit
Mbps	Megabits per second

TERM	DEFINITION
MB	Megabyte
MHS	message handling system
MHz	Megahertz
MMS	manufacturing message specification
Modem	modulator\demodulator
MOTIS	Message-Oriented Text Interexchange System
M-port	master-port
MS-DOS	Microsoft disk operating system
MTBF	mean time between failures
NCC	National Control Center
NACSIM	National Communications Security Information Memorandum
NCSC	National Computer Security Center
NDIS	Network Driver Interface Specification
NEC	National Electric Code
NetBIOS	Network Basic Input/Output System
NFPA	National Fire Protection Agency
NIC	network interface card
NIST	National Institute of Standards and Technology
nm	nanometer
NMS	network management system
NOS	network operating system
NRZ	non-return to zero
NSA	National Security Agency
OC	optical carrier
ODI	Open Data-Link Interface
OIW	Open Systems Implementor's Workshop
OLS	Optical Loss Set
OS	operating system
OSE	open systems environment
OSI	Open Systems Interconnection
OTDR	Optical Time Domain Reflectometer
PAD	packet assembler/disassembler
P/AR	peak-to-average ratio
PC	personal computer
PDN	packet data network
PDS	premises distribution system
PHY	physical layer protocol

TERM	**DEFINITION**
PLP	Packet Level Protocol
PMD	Physical Medium Dependent
PRI	primary rate interface
PVC	polyvinyl chloride
RAM	random access memory
RFI	radio frequency interference
RISC	Reduced instruction set computer
ROM	read-only memory
ROSE	Remote Operations Service Element
SIDPERS	Standard Installation/Division Personnel System
SMB	Server Message Block
SMC	Small Multiuser Computer
SMF	single-mode fiber
SMDS	switched multimegabit data service
SMT	station management
SNMP	Simple Network Management Protocol
SONET	synchronous optical network
S-port	slave-port
SSRC II	Standard Software Requirements Contract II
ST	snap twist
STP	shielded twisted-pair
TCP	Transmission Control Protocol
telco	telephone company
TIA	Telephone Industry Association
TMDE	test, measurement, and diagnostic equipment
TP	twisted-pair
TP4	transmission protocol-4
TPDDI	twisted-pair distributed data interface
TSB	Technical Systems Bulletin EIA/TIA
TSR	Terminate and Stay Resident
UHF	ultrahigh frequency
UL	Underwriters Laboratories
USAISEC	U.S. Army Information Systems Engineering Command
UPS	uninterruptible power
UTP	supply unshielded twisted-pair
WAN	wide area network

BIBLIOGRAPHY

Ronald O. Brown, "Choosing a LAN Architecture," (Networking Management, pp.58-62, December 1992)

Dave Powell, "Client/server: More than Packets and Protocols," (Networking Management, pp.28-31, January 1993)

William Stallings, "Data and Computer Communications," (Macmillan Publishing Company, 1988)

Bruce Berkoff and Max Schireson, "Electricity in the Air," (Corporate Computing, p. 121, November 1992)

Frank J. Derfler, Jr., "Guide to Connectivity," (Ziff-Davis Press, 1992)

Frank J. Derfler, Jr., "Guide to Linking LANs," (Ziff-Davis Press, 1992)

Paul J. Fortier, "Handbook of LAN Technology," (Multiscience Press, Inc., 1992)

Prepared by Office of Technical Assistance (OTA), GSA, "How to Buy Local Area

Networks," (U.S. General Services Administration, December 1991)

Richard desJardins, "How to GOSIP": OSI/GOSIP, Internets and Applications," (Interop Company, 1992)

Edited by John Bernaden and Richard Neubauer, "The Intelligent Building Sourcebook," (Johnson Controls, Inc., 1988)

Radia Perlman, "Interconnections, Bridges and Routers," (Addison-Wesley Publishing Company, Inc., 1992)

"Introduction to Local Area Networks," (Digital Equipment Corporation, 1982)

Thomas W. Madron, "Local Area Networks The Next Generation," (2nd edition, John Wiley & Sons, Inc., 1990)

Dann Derrick, "Network Know-How: Concepts, Cards & Cables," (McGraw-Hill, 1992)

Frank J. Derfler, Jr., "Linking LANS," p.183 (PC Magazine, Volume 12, Number 5, March 16,1993)

Jim Nash, "Peer Pressure," (LAN Magazine, pp.163-170, October 1992)

John Montgomery, "Power On!," (Corporate Computing, pp.117-120, November 1992)

Andy Feibus, "Reconstructing the Ultimate Server," (SCO Magazine, pp.32-41, January 1993)

"TCP/IP Defined," (Process Software Corporation, 1992)

TELETUTOR, Computer-Based Training Series, LAN: Local Area Networking, Appendix. Cooper and Associates Inc., Portsmouth, N.H., 1989.

☆U.S. GOVERNMENT PRINTING OFFICE: 1995 - 620-008/82016